



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DISSERTATION

**THE INSIDER THREAT TO CYBERSECURITY: HOW
GROUP PROCESS AND IGNORANCE AFFECT
ANALYST ACCURACY AND PROMPTITUDE**

by

Ryan F. Kelly

September 2017

Dissertation Supervisor

Shelley Gallup

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 2017		3. REPORT TYPE AND DATES COVERED Dissertation
4. TITLE AND SUBTITLE THE INSIDER THREAT TO CYBERSECURITY: HOW GROUP PROCESS AND IGNORANCE AFFECT ANALYST ACCURACY AND PROMPTITUDE			5. FUNDING NUMBERS	
6. AUTHOR(S) Ryan F. Kelly				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number NPS.2017.0024-IR-EP7-A.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) <p>The recent increase in high-profile insider cyber exploits indicates that current insider threat analysis (ITA) is insufficient to handle the growing insider threat problem. Well-established academic literature agrees that information overload is a problem ITA must overcome because ITA remains a human-intensive task. Two conceptual strategies to overcome information overload include reducing information and distributing information among additional people to accommodate the load.</p> <p>This dissertation applies attribution theory and process loss theory to test two ITA factors: ignorance and teamwork. A laboratory experiment with a convenience sample of 48 ITA-trained, top secret-cleared participants supported the research. Participants performed ITA with National Insider Threat Task Force training scenarios and applied the adjudicative guidelines for access to classified information. Teamwork conditions resulted in slightly higher accuracy at a significant cost of time, indicating that ITA analysts are best organized in different structures per informational and temporal constraints. However, ignorance level had little effect on ITA analyst accuracy. ITA analysts were substantially more accurate at implication scenarios but slightly better than chance at exoneration scenarios. Lower decision confidence associated with exoneration scenarios indicated that ITA analysts are more likely to guess when presented with an exoneration scenario. Further research involving larger independent samples and temporal constraints is necessary to verify these findings.</p>				
14. SUBJECT TERMS insider threat to cybersecurity, cybersecurity philosophy, attribution theory, process loss theory			15. NUMBER OF PAGES 303	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**THE INSIDER THREAT TO CYBERSECURITY: HOW GROUP PROCESS AND
IGNORANCE AFFECT ANALYST ACCURACY AND PROMPTITUDE**

Ryan F. Kelly
Captain, United States Army Reserve
M.B.A., Samford University, 2008
M.S., Naval Postgraduate School, 2014

Submitted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY IN INFORMATION SCIENCES

from the

**NAVAL POSTGRADUATE SCHOOL
September 2017**

Approved by:	Dan Boger Professor of Information Sciences Dissertation Committee Chair	Shelley Gallup Professor of Information Sciences Dissertation Supervisor
	Thomas Housel Professor of Information Sciences	Johnathan Mun Professor of Information Sciences
	Hy Rothstein Professor of Defense Analysis	

Approved by: Dan Boger, Chair, Department of Information Sciences

Approved by: Douglas Moses, Vice Provost of Academic Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The recent increase in high-profile insider cyber exploits indicates that current insider threat analysis (ITA) is insufficient to handle the growing insider threat problem. Well-established academic literature agrees that information overload is a problem ITA must overcome because ITA remains a human-intensive task. Two conceptual strategies to overcome information overload include reducing information and distributing information among additional people to accommodate the load.

This dissertation applies attribution theory and process loss theory to test two ITA factors: ignorance and teamwork. A laboratory experiment with a convenience sample of 48 ITA-trained, top secret–cleared participants supported the research. Participants performed ITA with National Insider Threat Task Force training scenarios and applied the adjudicative guidelines for access to classified information. Teamwork conditions resulted in slightly higher accuracy at a significant cost of time, indicating that ITA analysts are best organized in different structures per informational and temporal constraints. However, ignorance level had little effect on ITA analyst accuracy. ITA analysts were substantially more accurate at implication scenarios but slightly better than chance at exoneration scenarios. Lower decision confidence associated with exoneration scenarios indicated that ITA analysts are more likely to guess when presented with an exoneration scenario. Further research involving larger independent samples and temporal constraints is necessary to verify these findings.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	INSIDER THREAT ANALYSIS AND ANALYSTS.....	4
B.	RESEARCH PROBLEM	6
	1. Research Purpose.....	7
	2. Research Question	7
	3. Research Approach.....	7
C.	CONTRIBUTION.....	9
D.	ORGANIZATION	9
E.	SUMMARY	10
II.	LITERATURE REVIEW	11
A.	CYBERSECURITY	11
	1. Insider Threats to Cybersecurity	12
	2. Insider Threat Analysis	15
	3. Toward an ITA Theory	18
	4. An Information Science Approach to ITA	19
	5. Related Work	22
B.	COGNITIVIST PERSPECTIVE	24
	1. Attribution Theory.....	25
	2. Cognitive Load Theory	26
	3. The Taxonomy of Ignorance	29
	4. ITA References.....	33
C.	ORGANIZATIONAL THEORY	36
	1. Organizations as Information Processors.....	37
	2. Specialization Theory	40
	3. Process Loss Theory	43
D.	ITA PERFORMANCE MEASURES.....	48
E.	ANALYST CONFIDENCE.....	50
F.	SUMMARY	51
III.	EXPERIMENT DESIGN	53
A.	EXPERIMENT METHODOLOGY	53
	1. Research Design	54
	2. Procedure.....	54
	3. Experiment Apparatus	58
	4. Sample Justification.....	65
	5. Main Variable Operational Definitions	67

6.	Main Variable Attributes	68
7.	Blocking Variable (Demographics) Operational Definitions.....	77
8.	Blocking Variable (Demographics) Attributes.....	77
B.	JUSTIFICATION FOR LABORATORY EXPERIMENTATION	79
C.	SUMMARY	80
IV.	DATA ANALYSIS	83
A.	ANALYTICAL FRAMEWORK.....	83
1.	Primary Research Questions	83
2.	Analytical Methods	84
B.	DEPENDENT VARIABLE STATISTICAL CHARACTERISTICS.....	92
1.	Descriptive Statistics	92
2.	Correlation.....	94
C.	VALIDITY.....	95
1.	Threats to Internal Validity	95
2.	Threats to External Validity	97
D.	SUMMARY	98
V.	RESULTS	99
A.	ANALYST TIME.....	100
1.	Main Effects.....	100
2.	Interactive Effects	104
3.	Blocking Variable Effects.....	105
4.	Fixed Effects	105
B.	ANALYST ACCURACY	109
1.	Main Effects.....	109
2.	Interactive Effects	112
3.	Blocking Variable Effects.....	112
4.	Fixed Effects	113
C.	ANALYST PERFORMANCE.....	116
1.	Main Effects.....	117
2.	Interactive Effects	120
3.	Blocking Variable Effects.....	121
4.	Fixed Effects	121
D.	INFORMATION OVERLOAD PERCEPTION	122
1.	Main Effects.....	122
2.	Interactive Effects	124

3.	Blocking Variable Effects	127
4.	Fixed Effects	127
E.	SOCIAL-IMPACT PERCEPTION	127
1.	Main Effects.....	128
2.	Blocking Variable Effects.....	128
F.	CONFIDENCE.....	128
1.	Main Effects.....	129
2.	Interactive Effects	129
3.	Blocking Variable Effects.....	130
4.	Fixed Effects	131
G.	DISCUSSION	134
VI.	CONCLUSION	145
A.	METHOD	147
B.	CONTRIBUTION.....	148
C.	FINDINGS	148
1.	Attribution Theory Explanation.....	150
2.	Process Loss Theory Explanation.....	151
D.	SUMMARY	152
E.	RECOMMENDATIONS.....	156
1.	Enhance “Mitigating Factors” in the Federal Adjudicative Guidelines for Access to Classified Information.....	156
2.	Apply Attribution Theory to Computational Anomaly Detection	157
3.	Implement Horizontal Specialization in ITA Structure.....	158
F.	LIMITATIONS	159
G.	FUTURE WORK.....	160
	APPENDIX A. PERSONAL CORRESPONDENCE	163
	APPENDIX B. EXPERIMENT REPLICATION DOCUMENTS	167
A.	PARTICIPANT ASSIGNMENTS.....	167
B.	APPARATUS DESIGN	167
1.	Physical Configuration	168
2.	Server Configuration.....	168
3.	Participant Scenario Reference Relationship Matrix.....	172
C.	INSIDER THREAT SCENARIO OUTCOMES	174
D.	SURVEY INSTRUMENTS.....	176
E.	SUPPLEMENTAL.....	179

APPENDIX C. INSTITUTIONAL REVIEW BOARD.....	181
A. PAYMENT SCHEDULE	181
B. ANONYMOUS SURVEY CONSENT	182
C. PROTOCOL APPROVAL	184
APPENDIX D. ITA INFORMATION PROCESS.....	187
A. ITA CELL ORGANIZATIONAL ASSESSMENT	187
B. ITA ROLES AND RESPONSIBILITIES.....	189
1. Analyst	189
2. Case Manager.....	194
3. Enhanced Monitor	196
4. Cyber Operator	197
APPENDIX E. RESEARCH QUESTION STATISTICAL ANALYSIS.....	199
A. EXPERIMENTAL DATASET	200
B. DISTRIBUTIONAL FITTING.....	214
1. Tests of Normality	214
2. Tests of Homoscedasticity	221
C. DESCRIPTIVE STATISTICS.....	222
D. HETEROSKEDASTICITY, MICRONUMEROSITY, OUTLIERS AND NONLINEARITY.....	225
E. AUTOCORRELATION OF THE DEPENDENT VARIABLE AND DISTRIBUTIVE LAGS OF THE INDEPENDENT VARIABLES	226
F. TEST FOR NORMALITY AND SPHERICITY OF ERRORS.....	228
G. NONSTATIONARY ANALYSIS OF DEPENDENT VARIABLE	229
H. RESEARCH QUESTION ANALYSES.....	231
RESTRICTED VERSION OF THIS DISSERTATION.....	259
LIST OF REFERENCES.....	261
INITIAL DISTRIBUTION LIST	283

LIST OF FIGURES

Figure 1.	Interactive Time Effects—Teamwork vs. Ignorance.....	105
Figure 2.	Error Bar Chart—Time and Performance vs. Ignorance.	119
Figure 3.	Error Bar Chart—Time and Performance vs. Teamwork.	120
Figure 4.	Interactive Information Overload Effects—Teamwork vs. Ignorance. ...	126
Figure 5.	TS-Cleared Students with Insider Threat Training at NPS.....	163
Figure 6.	Personal Communication from National Insider Threat Task Force.	164
Figure 7.	KSE Screenshot—Scenario Stimulus.	168
Figure 8.	Entrance Survey.....	177
Figure 9.	Case Management Survey.....	178
Figure 10.	Exit Survey.....	179
Figure 11.	Analysis and Case Management Organizational Relationships.....	187
Figure 12.	Insider Threat Analysis Organizational Flow Chart.	188
Figure 13.	Performance Data Distribution.	216
Figure 14.	Time Data Distribution.	217
Figure 15.	Accuracy Data Distribution.	218
Figure 16.	Confidence Data Distribution.	219
Figure 17.	Information Overload Data Distribution.....	220
Figure 18.	Social Impact Data Distribution.....	221

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Research Design.....	8
Table 2.	Taxonomy of Ignorance. Source: Denby & Gammack (1999).....	30
Table 3.	Proposed Taxonomy of Ignorance Refinement.	32
Table 4.	Information Processing Contingency Matrix. Source: Tushman and Nadler (1978, p. 619).....	38
Table 5.	Relative Performance as a Function of Group Size. Source: Ringelmann (1913, p. 9).	44
Table 6.	Research Design.....	54
Table 7.	Relationship between Ignorance, Teamwork, and Scenario.	60
Table 8.	Entrance Survey.	63
Table 9.	Case-Management Worksheet.	64
Table 10.	Perceived Information-Overload and Personal-Performance Survey Items. Adapted from Soucek and Moser (2010).....	65
Table 11.	Perceived Social-Impact Survey Items. Source: Mulvey and Klein (1998).....	65
Table 12.	Participant Scenario and Reference Assignments.....	71
Table 13.	Independent and Dependent Variables.	85
Table 14.	Ancillary Research Questions, Variables, and Statistical Analysis Method.	86
Table 15.	Descriptive Statistics—Range, Mean, Standard Deviation, and Variance.	93
Table 16.	Descriptive Statistics—Skewness and Kurtosis.....	94
Table 17.	Correlation Matrix—Time, Accuracy, Performance, Confidence, Information Overload.....	94
Table 18.	Regression Analysis—Time vs. Ignorance.....	101
Table 19.	Mann–Whitney U Analysis—Time vs. Ignorance.....	101
Table 20.	Regression Analysis—Time vs. Teamwork.	103
Table 21.	Mann–Whitney U Analysis—Time vs. Teamwork.	103
Table 22.	ANOVA Results—Time vs. Scenario.	106
Table 23.	Kruskal–Wallis Test—Time vs. Scenario.....	107
Table 24.	ANOVA—Time vs. Scenario Outcome.	108
Table 25.	Mann–Whitney U Analysis—Time vs. Scenario Outcome.....	108

Table 26.	Logistic Regression Analysis—Accuracy vs. Teamwork.	110
Table 27.	Chi-Squared Test—Accuracy vs. Teamwork.	111
Table 28.	Cross Tabulation—Accuracy vs. Teamwork.	112
Table 29.	Logistic Regression Analysis—Accuracy vs. Age, Gender, Education, and Experience.	113
Table 30.	Logistic Regression Analysis—Accuracy vs. Gender.	113
Table 31.	Cross Tabulation—Accuracy vs. Scenario.	114
Table 32.	Regression Analysis—Scenario Outcome vs. Accuracy.	115
Table 33.	Cross Tabulation—Accuracy vs. Scenario Outcome.	115
Table 34.	Descriptive Statistics—Time, Accuracy, and Performance.	117
Table 35.	Kruskal–Wallis Test—Scenario vs. Performance.	121
Table 36.	ANOVA Results—Teamwork vs. Ignorance per Information Overload.	124
Table 37.	Regression Analysis—Analyst Confidence vs. Age, Gender, Education, and Experience.	130
Table 38.	Kruskal-Wallis Test—Confidence vs. Scenario.	132
Table 39.	Regression Analysis—Confidence vs. Scenario Outcome.	132
Table 40.	Mann–Whitney Test—Confidence vs. Scenario Outcome.	133
Table 41.	Cross Tabulation—Time and Accuracy per Outcome.	136
Table 42.	Supporting Research Questions, Analysis Method, and Results.	138
Table 43.	Hypothesis Test Results.	153
Table 44.	Participant, Scenario, Teamwork, and Ignorance Relationships.	167
Table 45.	Participant Scenario and Reference Assignments.	173
Table 46.	Experiment Dataset.	200
Table 47.	Insider Threat Analysis Case Summaries.	202
Table 48.	Distributional Fitting.	214
Table 49.	Tests of Data Distribution Normality.	215
Table 50.	Levene’s Test for Equality of Error Variances.	222
Table 51.	Summary Statistics.	223

LIST OF ACRONYMS AND ABBREVIATIONS

ACH	Analysis of Competing Hypotheses
ANOVA	analysis of variance
BBNM	Behavior-Based Network Management
CI	counter intelligence
CND	computer network defense
DOD	Department of Defense
GAO	Government Accountability Office
HR	human resources
ITAP	insider threat analysis performance
KSE	knowledge-sharing environment
MMOWGLI	massively multiplayer online war game leveraging the Internet
NITTF	National Insider Threat Task Force
OPM	Office of Personnel Management
RBAC	role-based access control
SA	security audit
SCI	sensitive compartmented information
SI	social intelligence
TS	top secret
UST	unbounded systems thinking
VRDM	Vector Relational Data Modeling

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

All acknowledgment belongs to the Holy Spirit, the Lord, the giver of all life, who, with the Father and Jesus Christ, comprise the one triune God of the Universe.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Once a science-fiction fantasy, cybercrimes are a quotidian worry in the 21st century; protections that were tech savvy only five years ago seem now as rudimentary as not leaving the key under the mat. Today, firewalls, intrusion detection systems, automated software patching, anti-virus software, and copious cybersecurity protections offer little more than a false sense of security to victims of cybercrime.

While the average hit is modest—perhaps an individual’s identity or a small business’s assets—sensational cyber megabreaches that affect thousands of people and cost organizations millions of dollars to rectify are now commonplace and, for many organizations, expected.¹ Overall, cybersecurity breaches cost an average of \$7.01 million per attack, a figure that increased 7% in 2016 alone (Ponemon, 2016), provoking a 35% increase in federal cybersecurity funding—which climbed from \$5.9 billion in 2007 to \$19 billion in 2017 (Fischer, 2016). Nevertheless, incidents are increasing steadily (Wilshusen, 2014), hits are ever harder to remedy, and defensive strategies are losing ground to ingenious workarounds. Despite their adherence to well-established cybersecurity practices, major corporations such as Target, Home Depot, eBay, and JPMorgan Chase have suffered severe incursions, illustrating that vulnerability is not merely the lot of the unsophisticated, careless, and naive.

The federal government is also inadequately defended, with notable victims including the Office of Personnel Management (OPM), Federal Bureau of Investigation, and Department of Homeland Security. These targets were well aware of the existential threat that insufficient cybersecurity posed, especially after 2013—a cautionary year in cybersecurity history due to the infamous Target breach. Yet the flaws and inadequacies of their systems were typically identified only after the damage was done. On average, breaches are identified ten months after the event; half are not intended as malicious, but stem from human error or glitches in the system (Ponemon, 2016).

¹ Cyber data breach liability insurance available at <https://www.thehartford.com/data-breach-insurance>; <https://www.travelers.com/small-business-insurance/data-breach-insurance>.

In other words, about 50% of breaches are caused by an insider, whether directly or indirectly, knowingly or not. The remaining 50% are attributable to an outsider (IBM, 2015). Of these breaches, phishing attacks comprise the highest share of reparation costs (33%; Roumani, Fung, Rai, & Xie, 2016). I categorize these attacks as insider in this work because successful phishing requires that insiders give away trusted network credentials. Regardless of the high proportion of insider causation, researchers overwhelmingly prescribe the same fatigued, outsider-oriented remedies in response—chiefly, variations on “defense in depth,” automatic software updates, and timely detection and response (National Science and Technology Council, 2016). The academic literature is replete with outsider-based diagnostics such as systems designed with insufficient security in mind, programmers validating code incorrectly, best practices neglected, and detection and response preferred over defense in depth. Progress in the security field is generally incremental, achieved by new spins on old concepts. This dissertation does not revisit external threat mitigation efforts, but rather charts a new direction by examining the little-understood problem of threats from within the system.

At first glance, insider threats to cybersecurity are a low base-rate problem. Snowden- and Manning-level breaches, though disastrous, are few and far between compared to traditional outsider attacks. Thus, the popular conception of a mainstream cybersecurity attack tends to exclude the idea of insider agency. In reality, however, when necessity and sufficiency are included, by definition, in the root causes of cyber-attacks, events that *lack* an insider threat component are rare. Take, for instance, the 2016 Democratic National Committee hack, wherein John Podesta gave his credentials in response to a phishing email, thereby acting as a cooperative insider. Cybersecurity systems are designed to grant access to those with legitimate credentials; the DNC’s system functioned correctly by doing nothing to stop the masquerade. The attacker relied on Mr. Podesta’s inside action and could not have succeeded without it.

While it is clear that cybersecurity breaches generally rely on some form of insider cooperation and system vulnerability for success, “insider threat” remains an ambiguous term. For instance, consider the Flame virus propagated through the Microsoft update service. The update service is implicitly trusted by millions of computer users,

rendering it a type of insider agent. The update service ought to be a sterling example of impregnable behavior. It has valid network credentials and automatic behavior far more predictable than that of its error-prone human organizational counterparts. And the action of the Flame malware is utterly contrary to the intentions of its developers and the expectations of Microsoft customers. But however robust and innocuous the update service is, it undeniably cooperated with the Flame virus to provide entree, without which the latter would be harmless. How, then, should the existential threat premise of Flame be classified: insider or outsider? Either answer must account for the relevance of the other, yet the traditional cybersecurity view is fogged by either/or.

Insider threats complicate the problem of defense. They transform the traditional (and comforting) view of cybersecurity from a well-defined problem—against which one might conceivably build a digital wall—into a messy conundrum with frustrating parameters that varies in solubility based on the information available to the analysts charged with seeking out insiders who threaten cybersecurity. Johnson, (2006, p. 82) offers that insider threats are problematic for cybersecurity because insiders are better positioned to explain away concerning behavior.

Insider threat analysts use available information to make causal attributions for observable behaviors. The absence of relevant available information introduces vulnerability in the form of “ignorance” defined as the lack of relevant knowledge or awareness. Insider threat analysts lack conclusive information with which to predict an insider threat in the making, because prediction denotes that the attack has yet to occur. Thus, insider threat analysis (ITA) differs from traditional forensics, in which network security analysts investigate a cybersecurity breach because, for the latter, the knowledge that there *was* a breach is sufficient to structure parameters for the problem.

ITA is poorly suited to algorithms and sensor triggers. The principle that “cognizance of the serious potential threat posed by information-system insiders should lead to complementary technical and nontechnical solutions” (McNamara, 2000, p. 84) is considered by the investigator as critical in ITA, which remains a mind-intensive task (Goldberg, Young, Memory, & Senator, 2016; Cappelli et al., 2012, p. 14). Regardless of value conveyed, the \$75 billion cybersecurity industry focuses primarily on technical

solutions that do little to counter the ubiquity of insider threats in systems whose controls, by design, allow access to anyone authorized. While the literature may describe insider threat–indicator ontologies and threat-actor taxonomies, studies pertaining to ITA are few.

A. INSIDER THREAT ANALYSIS AND ANALYSTS

The specialists most often needed to deal with internal threats are analysts and investigators. Analysts offer a nontechnical solution to insider threat mitigation, working to identify threats before an incident occurs and in many cases uncovering embryonic crimes during assessments. Investigators, by contrast, require, at minimum, reasonable suspicion of a crime having occurred before an investigation is launched.

Analysis is a mentally demanding task that requires the ability to see patterns in “apparent chaos” (Garst & Gross, 1997, p. 10). Garst and Gross and Cappelli et al. agree that information overload is the primary factor to overcome in creating order from information “chaff” (Cappelli et al., 2012, p. 196). Generally, there are two ways to reduce information overload: reduce the amount of information or add more workers to process the load. Drawing from well-established theories of structural contingency (Galbraith, 1977, p. 28; Thompson, 1967, p. 59–65; March & Simon, 1958, p. 158), Galbraith and Thompson identify horizontal specialization as a means to divide an information-processing task among several people so they can better accommodate the work. Task division requires an eventual reassembly that reduces productivity in the form of process loss. Specific to group work, process loss refers to a suboptimal performance effect that arises from inefficiencies in how the group works together (Steiner, 1966). A competing approach is to reduce the information an analyst must accommodate. There is presently no empirical research that demonstrates conclusively how either method affects analyst performance in terms of time, accuracy, and confidence. This dissertation seeks to fill the gap in research by organizing ITA analysts in horizontally specialized teams and as individuals to assess how each differs in analyst time, accuracy, and confidence under various information loads.

ITA may be sensitive to process loss because ITA work deals with processing ambiguous information. Problem solving with ambiguous information is difficult because such information is open to multiple interpretations. According to classic organizational theory, a group can approach a difficult problem-solving task by assigning parts to specialists to “almost certainly speed up the solution process and ... improve the quality of solutions” (March & Simon, 1958, p. 181). While this may hold true for programmatic tasks for which the solution is customized to fit a well-defined problem, there is scant research testing this proposition on uncircumscribed problems that lack a well-understood solution process.

An individual’s information-processing capacity varies with the complexity of the information presented. For instance, the letters “D,” “O,” and “G” are merely three units of information, unless there exists *a priori* a familiarity with the English word for canine, in which “DOG” is a single informational unit (Simon, 1996, p. 66). A lack of *a priori* context may exist when interpreting the ambiguous information inherent to ITA. Information-processing capacity may shrink disproportionately as the number of unfamiliar information units increases (Eppler & Mengis, 2004).

Threat analysts often employ up to 11 information sources (or references) in their work, including access and event logs, polygraphs, and user monitoring (Guido & Brooks, 2013; Brackney & Anderson, 2004). Increasing the number of references tends to be useful when investigating a known crime; the investigators can usually handle any number of references because they know what they are looking for (Jackson, 2014; Coffee, 2015). The same does not appear to hold true for threat assessments, in which analysts do not know if a crime has been, or will be, committed and must therefore sift through all available references in assessing threats (German & Stanley, 2007). Their lack of information or context creates ignorance, which varies depending on what references are available and in use.² Insider threat analysts must navigate multiple levels of ignorance to infer the existence of insider threats.

² Per Holtzman (1989) and Denby (1999), there are various levels of ignorance that alter how humans account for a lack of information in decision making. The greater the ignorance level, the less circumscribed a problem becomes because decision makers must accommodate unknowns within a decision system.

Under increased demand to predict and prevent crime, “federal, state and local governments are increasing their investment in fusion centers” (German & Stanley, 2007, p. 3). Fusion centers are intended to promote information sharing among federal agencies, and ITA hubs share a common purpose: assessing all available information to predict and prevent crime. However, fusion centers “are ineffective or provid[e] little value” (Coburn, 2015, p. 7), and the same may be true of ITA programs. The difficulty is that increasing the number of references and analysts involved in a task inevitably increases information load and coordination overhead, precipitating information overload and process loss (Steiner, 1972). Anticipating this problem, organizations tend to use specialization to overcome the cognitive limitations of personnel (Galbraith, 1977, p. 13). This tactic, despite funding boosts, has done little to decrease insider threats. The problem requires new focus; the alternative lens of organizational-contingency theory offers insights into real contexts and constraints, and a platform on which to build new solutions (Galbraith, 1977, p. 28).

B. RESEARCH PROBLEM

Insider threats are an ever-changing problem, eluding detection (Oltsik, 2013; Internet Crime Complaint Center, 2014) and contributing to a range of harmful and devastating blows such as intellectual property theft and unauthorized disclosure (Proudfoot, Boyle, & Schuetzler, 2016; Axelrad & Sticha, 2013; Baracaldo & Joshi, 2013; Chinchani, Iyer, Ngo, & Upadhyaya, 2005). ITA is a human-intensive task that requires alert interpretation of acontextual information (Goldberg, Young, Memory, & Senator, 2016; Cappelli et al., 2012, p. 14). Information overload is a known problem for ITA (Cappelli, et al., 2012, p. 196; Garst & Gross, 1997). Reducing information or dividing information processing tasks between teams of people are methods to overcome information overload but the effects of implementing either solution in an ITA task are not conclusive. Ignorance, or a lack of contextually relevant information, is inherent in ITA—it cannot be exorcised. A serious gap in the cybersecurity research is the lack of empirical evidence by which to understand how teamwork and ignorance affect insider

threat assessments.³ In the absence of this data, we do not know how best to organize insider threat analysts as they work under various information constraints.

1. Research Purpose

The lack of applicable theory that describes, explains, and predicts performance leads many to share the view that ITA is more an art than a science (Utin, 2008, p. 168; Sellen, 2016; Wittcop, 2017). The purpose of this dissertation is *to demonstrate the controllability of ITA by manipulating conditions of teamwork and ignorance and measuring insider threat analyst performance in terms of accuracy and time*. This is important because this research provides evidence that ITA is scientifically understandable and analyst time and accuracy are experimentally controllable. This dissertation applies attribution theory, a product of cognitive psychology, to evaluate how analysts collectively and individually make attributions in various levels of ignorance. Process-loss theory, a product of organizational theory, is applied to the cognitive dynamics of teamwork to explore ITA as a specific use case. Test results are examined to suggest principles for ITA organizational approaches under various informational constraints.

2. Research Question

This dissertation research emerges from the general question, “Is insider threat analyst performance controllable?” Theories of attribution and process loss hold promise in applying two key factors, ignorance and teamwork, that may affect performance, measured as productivity within a given time. Thus, the specific research question studied in this dissertation is, “How do ignorance and teamwork affect analyst accuracy, time, and confidence?”

3. Research Approach

This research tests attribution and process-loss theory as applied to ITA by means of a *laboratory experiment that varies two levels of ignorance under two conditions of*

³ This research defines ignorance levels according to Denby & Gammack’s (1999) taxonomy covered in Chapter II. This work tests two levels of ignorance, high and low, that loosely relate to “Gordian” and “Watsonian” ignorance, respectively.

teamwork and measures how each affects analyst accuracy, time, and confidence. Ignorance is operationalized as “high” and “low.” Teamwork is operationalized as “horizontally specialized” and “none.” The experiment measures the social impact and information-overload effects operationalized as two dependent measures: “perception of information overload” and “perception of social impact.”

The theoretical relationships between the research constructs fit well within a two-by-two factorial design. Bowing to Kerlinger and Lee (2000, p. 225),

there is something salutary about reducing a research problem to a crosstab. In fact, if you cannot write a diagrammatic paradigm of your research problem in either analysis of variance or crosstab form, then the problem is not clear in your mind, or you do not really have a research problem.

Crosstabs are employed to provide a framework for examining interactive effects clearly and intuitively. The experimental design considers the effects of various conditions of teamwork and ignorance on accuracy, time, confidence, information overload, and social impact, as presented in Table 1.

Table 1. Research Design

		Ignorance	
		High	Low
Teamwork	Horizontally specialized	Accuracy Time Confidence Information overload Social impact	Accuracy Time Confidence Information overload Social impact
	None	Accuracy Time Confidence Information overload	Accuracy Time Confidence Information overload

C. CONTRIBUTION

A dense body of research describes an interaction between organizational structure and task performance wherein process loss occurs when problems are solved collectively. A typical experiment generally evaluates the role of these concepts in a clearly defined task such as rope pulling (Ringelmann, 1913), LEGO-man assembly (Staats, Milkman, & Fox, 2012), research-model development (Schippers, 2014), and crisis mapping (Mao, Mason, Suri, & Watts, 2016). Staats et al. provide evidence that additional workers can decrease performance after some optimal point, but Mao et al. demonstrate that adding workers increases performance. This discrepancy arises for two reasons: the workload was not the same for the teams, and Mao et al.'s experiment required little interdependence. These experiments set unambiguous parameters by assigning participants a task with an expected outcome that is known to the participants beforehand. The experiments do little to assess team dynamics for tasks that involve participants who must solve problems given acontextual information. By contrast, this research evaluates the performance of teams and individuals in solving more ambiguous problems—specifically, insider threat analysis.

In evaluating how teams and individuals perform causal attributions under various levels of ignorance, this work extends the field of attribution theory.⁴ By focusing on the number of available references as a factor of information load, I follow a research challenge on overload factors in real-life contexts (Jackson & Farzaneh, 2012). The findings of this research illuminate how insider threat analysts perform under various organizational and informational constraints.

D. ORGANIZATION

Chapter II of this dissertation synthesizes relevant literature on specialization, attribution, process loss, social impact, information overload, and introduces the philosophical underpinnings of the present work. Chapter III discusses research design, experimental apparatuses, the criteria for participant selection, and analytical framework.

⁴ The theory of attribution states that people will search for the reason that certain events occur when the cause is hidden. Attribution theory is covered in more detail in Chapter II.

I present a unique means of simultaneously assessing the effects of teamwork and ignorance via a two-by-two factorial design. This work outlines data-analysis methods in Chapter IV and addresses threats to internal and external validity. Findings are reported in Chapter V; Chapter VI concludes with implications, limitations, recommendations for improved insider threat analyst performance, and suggestions for future research.

E. SUMMARY

This introduction presented a brief background of the insider threat to cybersecurity. The chapter cited relevant research that suggests information overload is a problem for insider threat analysis. Two methods of reducing information overload followed: reduce the information, and distribute the load among additional people. Information reduction makes ignorance a testable construct and information distribution makes teamwork another testable construct. Both methods of managing information overload have performance implications predicted by well-established theories of attribution and process loss that this dissertation subjected to empirical testing. This work organized the constructs within a two-by-two factorial design with five dependent measures: time, accuracy, confidence, perception of information overload, and perception of social impact. This chapter concluded with the scientific contributions of this work and a brief summary of how this dissertation is organized.

II. LITERATURE REVIEW

This chapter provides a background of the insider threat to cybersecurity and focuses on theories of attribution and organizing. The work surveys current literature that offers the reader a definition of insider threats and a description of insider threat analysis. The work reviews well-established science philosophy and offers information science as a tool to better describe, explain, and predict analyst performance.

This chapter first surveys the insider threat literature and identifies a theoretical concept, information overload, as a problem for ITA to overcome. The work then reviews ignorance, or reducing relevant information, as a conceptual method to overcome information overload; as an alternative, theories of organizing offer teamwork as a method for distributing information load between people. The work continues with effects of ignorance predicted by attribution theory and effects of teamwork predicted by process loss theory. The review describes how ignorance and teamwork affect ITA in terms of performance, namely time and accuracy. This literature review subsequently presents relevant research used in Chapter III to operationalize ignorance, teamwork, and performance, and concludes with eight testable hypotheses drawn from the literature.

A. CYBERSECURITY

Outsider cyber threat analysis, herein referred to as “computer network defense” (CND), uses a deductive–analytic inquiry system to identify network exploits. Cybersecurity personnel can use deductive–analytic inquiry because they identify specific malicious indicators after known attacks; they then submit the indicators to published reputation lists (Sanders, Randall, & Smith, 2014, p. 176). The indicators generally involve a set of recognizable patterns uniquely identified as signatures. Network-protection hardware and software, including insider threat detection software, use signatures to recognize cyber threats (Sanders et al., 2014, p. 204). Because signatures identify known threats only, contemporary cybersecurity methods tend to follow the “detect and respond” paradigm. “Detect and respond” reduces reliance on prevention by increasing human analysis and active responses (Schwartau, 1999, p. 36). This shift in the way of

cybersecurity thinking balances traditional “defense in depth” with human analysis. Both methods allow authorized access by design and view cybersecurity from an outsider perspective. Insiders with authorized access do not fit within this CND analytical domain, and detecting their risky behavior requires a different way of thinking.

Insider threat analysts use an inductive–consensual inquiry system to identify potential attackers. Insider threat analysts must resort to inductive-consensual inquiry because deductive rules do not work with insiders due to the variable contexts underpinning insider behavior. Inside attacks differ from outside in that outsiders are more easily detected as intruders when their means of access are found to be illegitimate. Insiders have authorized access already and can “more easily justify or explain away their activities” (Johnson, 2006, p. 82). Insiders can also redirect suspicion; an example is those who are best positioned to detect deceivers are constrained by pre-emptive retaliatory discrimination accusations and whistleblower program abuses in order to deflect attention from the insider threat to the person who may detect them (Catrantzos, 2012, p. 117). Furthermore, insider threats need not necessarily be malicious (Hunker & Probst, 2011).

Insider threat experts present insider threat indicators such as “financial and personal stressors” as factors for ITA (Silowash, Cappelli, Moore, Trzeciak, Shimeall, & Flynn, 2012, p. 29). Such indicators are not signatures because they do not deduce insider threats. Signature-based protection alone is not effective against this range of internal threats, because such threats do not have signatures (Cole & Ring, 2006, p. 20). Analysts use a combination of lessons learned from past cases and specified indicators to assign behaviors meaning so they can better identify insider threats (Cappelli, Moore, & Trzeciak, 2012, p. 196; Faber, 2015).

1. Insider Threats to Cybersecurity

Insider threats are essentially agents of an organization with a propensity to harm the organization. This definition includes trusted impostors, negligent non-malicious trusted people, and trusted software. Established theories of organization posit a fit among people in the organization and its structure, technology, and inputs and outputs (Nadler, Tushman, & Hatvany, 1980; Galbraith, 1977; Leavitt, 1965). The organization is

less an entity per se than an artificially constructed relationship among entities. Organizations emerge when shared beliefs create a pattern of labor divisions that collaborate toward a purpose (Galbraith, 1977, p. 3), and good organizations have parts that interact to achieve this common purpose (Ashby, 1962, p. 111). Thus, an agent who is not working toward the common purpose does not fit well in the organizational structure and may be a threat.

When insider threat problems are approached from a CND perspective, a fundamental translation problem emerges with how CND and ITA analysts communicate with each other. CND analysis is data centric, with a focus on collection and network heuristics (Sanders et al., 2014, p. 11; Bejtlich, 2013, p. 9). By contrast, ITA is not centered on network data, but focuses on perceiving the *context* of behaviors (Cappelli et al., 2012, p. 14). The ITA and CND communities may appear similar because cyber-attackers generally gain access to a system by masquerading as authorized inside users. ITA and CND personnel may both work to protect the same network information, but they live, work, and communicate in different worlds.

It is well established in network security theory that network defenses will eventually fail (Sanders et al., 2014, p. 7; Schwartz, 1999, p. 26). While the current best practice is to learn from past attacks to identify similar instances in the future, cyber-attacks need be successful only once to exact irrecoverable damage (Cappelli et al., 2012; FireEye Inc., 2013). For this reason, cybersecurity theory tends to organize attacks according to an eight-step method (McClure, Scambray, Kurtz, & Kurtz, 2012), with a corresponding “intrusion kill chain,” as a cyber-defense methodology (Hutchins, Cloppert, & Amin, 2011, p. 3). The problem with a CND-centric viewpoint is that attackers generally use automated attack methods that overwhelm the human capacity for timely response—92.9% of system-compromising attacks happen in a matter of minutes (Verizon Inc., 2016). Having compromised a system, the attacker generally operates with impunity; but if cyber-defense includes an insider threat component, it is possible to command greater control over the targeted space.

Insiders can be expected to operate in a predictable manner because they are a part of an organizational design. That is to say, we may not know how or when an intruder

gains access, but we should be able to tell an outsider's network identity from a proper insider's because the outsider will behave differently than we expect of an insider. Likewise, many researchers agree that anomaly detection is an integral component for insider threat analysis (Brdiczka, Liu, Price, Shen, Patil, Chow, Bart, & Ducheneaut; 2012; Young, Memory, Goldberg, & Senator, 2014; Gavai, Sricharan, Hanley, Signhal, & Rollerson, 2015; Sanzgiri & Dasgupta, 2016). Recent advances in user entity behavior analytics (UEBA) software claim to detect behavioral anomaly, but the technology does not eliminate the need for human analysis (Armerding, 2015). Human insider threat analysts determine if anomalous inside network behavior, if not otherwise explained, is a threat.

It is useful to apply an insider threat lens to all cyber-attacks because attackers generally gain access and operate as authorized users. Nearly one-third of breaches are directly attributable to insiders and nearly two-thirds use legitimate credentials to access the victim network (Net Diligence, 2015). High-profile cyber-attacks tend to be insider jobs. The hack of the Ashley Madison website, for example, is thought to have been perpetrated by an insider (Symantec, 2016). In the 2013 Target breach, credentials from a trusted third party—a heating and air conditioning subcontractor—were used to install malware on point-of-sale devices. Attackers also leveraged stolen credentials from a trusted third party for access in the OPM breach, and, in turn, OPM staff acted as insider threats themselves when they failed to properly secure sensitive data according to industry standards and federally promulgated policy. OPM cybersecurity staff did not exploit vulnerability but their negligence exposed OPM's data to hackers. A congressional report on the breach indicated that OPM's people, not cybersecurity technology failures, were to blame for the breach because there was a discernible pattern of negligence that left the agency vulnerable to attack. According to the Committee on Oversight and Government Reform, "had OPM implemented basic, required security controls ... when they first learned hackers were targeting such sensitive data, they could have significantly delayed, potentially prevented, or significantly mitigated the theft"; the Committee went on to state that "the longstanding failure of OPM's leadership to implement basic cyber hygiene, such as maintaining current authorities to operate and employing strong multi-factor authentication, despite years of warnings from the

Inspector General, represents a failure of culture and leadership, not technology” (Chaffetz, Meadows, & Hurd, 2016, p. ix). These examples indicate that cybersecurity should include an insider perspective because guards, though present for duty, introduce vulnerability in the form of illusory security when sleeping on the job.

2. Insider Threat Analysis

Insider threats to cybersecurity are pervasive; no lock can keep out one who holds the key. There is no universally accepted definition of an insider threat, but the literature contains common themes. According to Cappelli et al. (2012), insiders are people; Bishop et al. (2014, p. 253) describe an insider as an “activity execution agent,” whether a person or a program; Pfleeger, Predd, Hunker, and Bulford (2010) assert that insiders are the actions of a threat actor, as distinct from the physical actor himself. In this sense, authorized actions can be threats when performed by an actor who has good intentions and diligence, but commits harmful acts. All concur, however, that insiders have some kind of authorized access with sufficient privilege to put an organization’s data, processes, or resources at risk. Some authors argue that insider threats involve malice (Schultz, 2002; Cole & Ring, 2006, p. 7), whereas others include unintentional negligence (Hunker & Probst, 2011; Contos, 2006, p. 149). Hunker and Probst (2011) conclude that actors can be impostors who do harm through authorized access. The Department of Defense (DOD) adds any threat of espionage, terror, unauthorized disclosure, and sabotage, regardless of intent (Department of Defense[DOD], 2014), to the definition. All agree that insider threat actors are trusted agents with the propensity to harm.

The inevitability of risk associated with trusted agents, expressed by the ancient dilemma, *quis custodiet ipsos custodes?* remains a serious problem. Attacks may cause irreparable damage, subject to little remedy, before law enforcement officials are aware (Cappelli et al., 2012; Contos, 2006; Cole & Ring, 2006).⁵ Traditional enforcement measures can do little to defend against insider threats because investigations commence after the offense. Meanwhile, the emergence of new forms of anti-stalking laws, school-

⁵ *Quis custodiet ipsos custodes* is a Latin phrase from the Roman poet Juvenal’s Satire IV, line 347 translated as “Who watches the watchmen?”

safety legislation, and restraining orders suggests a movement toward identifying would-be culprits proactively.

The insider threat literature is inundated with taxonomies of actors and ontologies of indicators, but little attempt is made to research the analysts whose job is to seek out these threats. Insider threat analysts may synthesize many references to detect when an insider is not behaving as expected and infer if that behavior presents a risk. An investigator follows up on the threat analyst's inference using deductive reasoning to determine if the insider identity is a security risk or an impostor, or if there is a legitimate explanation for the unexpected behavior. These analysts attempt to identify malevolent inside actors before they can use privilege to do harm—that is, they watch the watchmen. They do so by identifying and validating behavior that has a propensity for harm.

Gary Kline's (1998) recognition-primed decision making concept provides a theoretical basis that insider threat analysts' intuition must be informed by some foundational precepts. Incidentally, there are 13 “adjudicative guidelines for determining eligibility for access to classified information” that define risky behaviors (Adjudicative Guidelines, 2016; Carney & Marshall-Mies, 2000). The guidelines, however, are not deductive rules; they are subjective in nature. For instance, each guideline has “conditions that *could* raise a security concern and *may* be disqualifying” with each accompanied by “conditions that *could* mitigate security concerns” (Adjudicative Guidelines, 2016, p. 530; emphasis added). The guidelines note that conditions themselves are also subjective such as “conduct which *may* make the individual *vulnerable* to coercion, exploitation, or pressure” (emphasis added). This absence of well-defined parameters is why humans, instead of computers, are required to perform insider threat analysis.

The human-dependent nature of ITA commonly surfaces in operational settings. A contemporary example is how a popular insider threat software title flagged user activity that matched “.ru,” the top-level Russian domain. The software found “**ru** 4 realz?” a phrase that did not imply involvement with Russian content; software analytics would conclude the same. However, the human analyst investigated what he interpreted

as a use of juvenile language and discovered that the insider was soliciting a minor for illicit sexual behavior. Indicators that lack explicitly programmed instructions for computer software go unseen if not for human analysis. Thus, humans must contextualize ambiguous behaviors and determine if violations of the adjudicative guidelines exist.

ITA requires different skills than those required for an investigation because the nature of the problem differs. ITA problems tend to be messy, and the difficulty of solving them increases geometrically as ignorance is introduced into the analysis. Ambiguity tends to make ITA indivisible into a smaller, more manageable problem. Problems that have better-defined parameters tend to be more structured, increase in difficulty linearly with complexity, and are divisible. For example, a typical children's wood block puzzle may be solvable with or without the puzzle frame. The puzzle frame bounds the problem, informs the expected outcome, and allows deductive analytics, thus simplifying the solution. When using the puzzle frame, a child knows if he has the correct number of pieces and can deduce the solution is correct. Given the same puzzle pieces with no bounding frame, he proceeds by examining the relationships among the pieces and infers a most likely correct solution based on his predicate knowledge. In this case, the puzzle solver uses abductive reasoning—that is, he transitions from observation to theory, using the simplest and most likely explanation—so there is no guarantee of truth. He does not know if he has all the pieces, or too many or unrelated pieces. If he has no relevant knowledge of the expected solution, it is likely he will not be certain of a correct solution if he sees it. He determines that the problem has been solved correctly when the pieces seem to fit together or the outcome looks right based on his predicate knowledge.

In life and science, a set of observations may permit many consistent explanations (Lombrozo, 2007), but the best explanation may be insufficient to establish a premise of truth, which requires that the explanation be both necessary and sufficient (Musgrave, 1988; Lipton, 1993). That is to say, an explanation should posit a cause that can account for the effect observed, and that cause should be sufficient in itself to produce the effect. Fein and Vossekuil (1998) expand upon Musgrave and Lipton's views, offering three assumptions that underpin threat assessment: the behavior must be discernible, a link between past behaviors and a potential attack must exist, and an interaction between

actor, environment, and target must be evident. Fortunately, inside actors are known to leave a trail of evidence before a breach that demonstrates interactions among actor, environment, and target (Baracaldo & Joshi, 2013; Brdiczka et al., 2012; Cappelli et al., 2012; Moore, Cappelli, & Trzeciak, 2008). Thus, *a priori* identification of insider threats is theoretically feasible, given sufficient information.

3. Toward an ITA Theory

Scientific theories shape our understanding of world phenomena (Thagard, 1993, p. 33). According to Ruben (1975, p. 66), there is no scientific theory without order, and all theory assumes the world is rationally ordered to some degree. Theories comprise interrelated constructs, propositions, and definitions that explain phenomena with meaningful representations by specifying the relationships between constructs (Kerlinger & Lee, 2000, p. 64). According to Creswell (2014, p. 54), a theory may appear as an “argument, discussion, figure, or rationale” that explains phenomena. The building blocks of this rationale are presented in Feigl’s (1970) “orthodox view” diagram, which illustrates constructs linked to observations, and vice versa. Ronald Giere’s (1991, p. 32) model of a scientific episode similarly describes these links as relationships between four elements: real world, model, data, and prediction. Following Giere’s interpretation, a model is a theory that should conform to some particular aspect of the real world that we observe as data. If the model is correct, the prediction should agree with the data; this gives data meaning and enables prediction in the real world. To Giere, agreement between the real world, model, data, and predictions displays the power of a theory.

To say a theoretical model is true is to say that it has some correspondence with the real world (Godfrey-Smith, 2003, p. 188). Rudolf Carnap (1956) asserts that all observations can be defined in theoretical language through what he calls “rules of correspondence.” To Carnap, the observable (a measurable relationship between mass and temperature) is more meaningful than the unobservable (speculative metaphysics), and correspondence truth theories suggest that there is some direct empirical observation that provides evidence of truth. Observation has its limitations, however, chiefly to do with predicate knowledge, and observational language cannot communicate an

understanding of theoretical terms (Hesse, 1970). In other words, two people can see the same object from the same viewpoint, but based on their prior knowledge they will experience the object differently because observation is an activity of the mind more than the eye (Hanson, 1958). Therefore, this research draws on the broad theoretical domain of cognitive psychology to investigate insider threat analysis.

4. An Information Science Approach to ITA

Current investigations seek to predict the behavior of a cyber-attacker via computer programs that identify evidence of an attack based on known predications. A cyber threat that exploits a system in an expected way should thus be detected; yet threats that act unexpectedly subvert cyber-defenses and must be watched for. David Hume's philosophy might see the cyber security problem as a "matter of fact" and the insider threat problem as a "relation of ideas" (Hume, 2004, p. 14). When new threat vectors are exploited, cyber-defense analysts are incapable of predicting the cause because conception *a priori* is more a matter of chance than recognition. Much of the problem with causality is what Hume calls a problem with induction. To Hume, "it is impossible to discover causes and effects for any new observation, and any supposition thereon is completely arbitrary" (Hume, 2004, p. 17). Consistent with these insights, a recent Government Accountability Office (GAO) report reveals that cybersecurity comes short in "identifying root causes of issues" (Goldenkoff, 2015, p. 18).

Hume's philosophy on inductive reasoning explains the limits to identifying unknown threats. Pedro Domingos framed the induction problem in his 2015 book *The Master Algorithm* with the question, "How can we ever be justified in generalizing from what we've seen to what we haven't?" (p. 58). Threat assessment strategies such as profiling, automated decision making and guided professional judgment are at least three methods that attempt to accommodate the demands of threat assessment (Reddy, Borum, Berglund, Vossekuil, Fein, & Modzeleski, 2001). Of these, guided professional judgment is the only strategy that suggests a move from a deductive–analytic inquiry system to one that allows for multiple perspectives.

Ian Mitroff, an expert on unbounded systems thinking (UST), echoes Hume by stating that neither method (agreement or analysis) can establish “one of the most fundamental principles in science—causality” (Mitroff & Linstone, 1993, p. 86). He goes on to present both the consensual and analytical as components of the “technical perspective” (p. 97), which proceeds from an objective epistemology because it perceives the meaning of things as they exist independent of the mind (Crotty, 1998, p. 5). A more complete view would include additional perspectives, as digital data are only a partial contribution to understanding the overall picture (Johnson, 2006, p. 176). The UST approach seeks to balance the technical perspective with organizational and personal perspectives (Mitroff & Linstone, 1993, p. 107). The approach fits ITA because it interrelates three perspectives—the objective (technical), constructivist (organizational), and subjective (personal)—into a single inquiry system that offers a more complete way of knowing (p. 99).

Insider threats urge a UST approach to a messy, multifaceted problem. Threat actors exhibit identifiable behaviors that should indicate an existing latent threat; in retrospect, the same indicators are components in an investigator’s trail of evidence. Many indicators can be used to bring an event into context when examined through technical, organizational, and personal perspectives. For instance, network activity (a technical indicator), personnel duties and roles (an organizational indicator), and financial status (a personal indicator) may collectively identify an insider threat, manifest an imposter, or exonerate an innocent party; individually, however, they offer insufficient information.

Insider threat analysts assess information from multiple sources to identify sequences of events that suggest suspicious behavior (Faber, 2015). While computer sensors can generate data at an overwhelming rate that is difficult to manage (Jackson & Farzaneh, 2012; McAfee, Brynjolfsson, Davenport, Patil, & Barton, 2012), new big data technologies make the data more manageable to human counterparts—at the cost of context (Wang, 2013). Humans can reassign meaning to the data in a given context *a posteriori* because of their ability to continuously adapt to environmental changes (Simon, 1996, p. 53). For instance, a quote from a celebrity figure may mean something entirely different if spoken by a politician, and humans will intuitively discern the meaning based on the

quote's context. Rule-following computers are incapable of this adaptation due to variations in contextual relevance (Gordon, 2016; Dreyfus & Dreyfus, 1986). According to Dreyfus and Dreyfus, computers suffer from a "common sense" problem (p. 79).

It follows, then, that humans are at some point necessary to interpret the data required to perform an effective analysis (Goldberg et al., 2016; Sanders et al., 2014, p. 13). There are, however, known limitations to human information-processing capacity (Simon, 1996, p. 81). As a result, humans introduce vulnerability in the form of information overload (Shenk, 1997; Oppenheim, 1997; Kirsh, 2000). The robust body of research on information overload (for example, Jackson & Farzeneh, 2012; Klausegger, Sinkovics, & Zou, 2007) generally describes the phenomenon in terms of time (Schick, Gordon, & Haka, 1990), information complexity (Edmunds & Morris, 2000), and individual information-processing capacity (Eppler & Mengis, 2004; Simon, 1996).

Time, information complexity, and information-processing capacity may be related in ITA analysis much as time, quality, and cost are related in the theory of constraint (Goldratt & Cox, 2016); as information complexity increases and time is held constant, information-processing capacity must also increase. Human limitations in information-processing capacity explain much of the problem with contemporary cybersecurity (Simon, 1996, p. 87).

The intersection between computer data and human information is a crucial point of investigation, involving aspects of human information behavior. There is consensus that the study of human information behavior should have primacy over programmatic information behavior in such studies (Spink, 2000; Bates, 1999). Computers are programmed, and thus computer information behavior is an engineering task. Human information behavior, on the other hand, is not programmatically defined; it must be understood first, and computers subsequently programmed to interact with the information appropriately. Understanding human information behavior is, in this sense, the result of a competent scientific inquiry of information (i.e., a science of information).

Information science is an appropriate avenue through which to study cybersecurity because it is an interdisciplinary science that examines unseen forces

governing both manual and mechanical techniques of information use (Taylor, 1966), especially the properties, storage, movement, and processing of information for optimal utility (Zins, 2006; Borko, 1968). Examining those forces that govern the optimal flow of information, specifically between computer data and the cybersecurity personnel who process them as information, lies firmly within the bounds of information science.

5. Related Work

Fraud theory research is a closely related thread of work (Dorminey, Flemming, Kranacher, & Riley, 2012). Donald Cressey's seminal work with the "fraud triangle" in 1953 provided three necessary but not individually sufficient conditions for accounting fraud. According to Cressey, "trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware that this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conception of themselves as users of the entrusted funds or property" (1953, p. 30). Cressey claimed that violations of trust required a minimum of some non-shareable problem, opportunity, and rationalization.

To Cressey, the very conception of fraud in the mind of a trusted agent defines that agent as a trust violator. Under Cressey's conceptualization, cyber penetration testers would be trust violators, as would anyone who understands a financial accounting system well enough to exploit it undetected and conceives a notion to do so, regardless of his integrity. Such a violation is not observable with the disputable exception of a polygraph examination.

Many scholars expanded on Cressey's work (Schuchter & Levi, 2013; Kassem & Higson, 2012). Wolfe and Hermanson's (2004) work changed the triangle to a quadrangle with the addition of capability. The "fraud diamond" included four conditions for accounting fraud: incentive, opportunity, rationalization, and capability. Wolfe and Hermanson agree with Cressey that a rationalization component assumes there is some inner voice that must be overcome to commit fraud. Albrecht (1984) replaced

rationalization with integrity, theorizing that poor personal integrity is a condition that suggests higher fraud risk. While the model makes sense, neither rationalization nor integrity is readily observable unless the insider has a documented history of crime.

Kranacher, Riley, and Wells's (2011) "money, ideology, coercion, ego" (MICE) model expanded Cressey's "problem" component into a four-part model with a multi-perspective "ideology" component. According to Kranacher et al., ideology can motivate fraud without desire for personal gain—for instance, the loan officer that clandestinely modifies a loan document so he will not be forced to evict a single mother and her eight young children after her husband, the sole breadwinner, was killed in combat while fighting for all citizens—including the bank employees—freedom. Ideology in this sense would negate rationalization, at least in the sense that the behavior is wrong from the loan officer's perspective.

Perspective fundamentally changes how predicate fraud elements are understood. From a cybersecurity standpoint, opportunity for the fraudster is the same thing as vulnerability for the organization he attacks. Furthermore, fraud is only one type of insider threat. The fraud triangle is used to assess the risk of financial fraud to help financial organizations better predict fraud (Morales, Gendron, & Guenin-Paracini, 2014). According to Cappelli et al. (2012), insider threats can also be saboteurs, spies, and information thieves. In this sense, the fraud triangle will do little to predict nation-state cyber espionage.

Richards Heuer's (1999) Analysis of Competing Hypotheses (ACH) is an eight step method developed through the Central Intelligence Agency to help intelligence analysts overcome confirmation bias and other analytic shortcomings. The ACH framework requires that an analyst list all possible explanations to answer a question when information is unavailable for certainty. Using this method, an analyst can logically exclude unlikely explanations by organizing the explanations and evidence *against* each explanation in a tabular format. Analysts must ignore evidence that confirms any explanation and as a result, the explanation with the least evidence against it is the most likely explanation. Failure to find evidence against several explanations does not prove the explanations, but rather indicates that additional information is necessary to disprove

multiple explanations until there is one *most likely* remaining. A problem with the ACH method is that analysts must conceptualize explanations *a priori*. However, in reality, threat analysts must put anomalous behaviors into context in order to identify if an insider is a threat before following up with an investigative method such as the ACH.

The fraud triangle and the ACH methods are tools that investigators may use to infer genuine insider threats after identified by analysts. Opportunity, rationalization, and pressure loosely relate to the means-motive-opportunity trifecta established in criminal proceedings. Nick Catrantzos offers another similar trifecta, the “target, open door, and a dark corner” method of insider threat assessment (Catrantzos, 2012, p. 3). Catrantzos’s method focuses on the environment and intent rather than the work of the insider threat analyst. Certainly there are more methods for assessing risk, and this research does not intend to juxtapose them. Rather, this research examines how teamwork and ignorance conditions affect insider threat analysis performance.

B. COGNITIVIST PERSPECTIVE

The way an analyst discerns insider threats depends upon the psychology-based tools the analyst employs. Paradigms that could explain insider threat analysts’ processes include behaviorism, constructivism, and cognitivism. Behaviorist learning theories are based on stimulus–response associations that do not involve the role of memory (Ertmer & Newby, 2013). A behaviorist learning theory may be appropriate for cyber network defense (e.g., responding a certain way to known malicious signatures), but it does not work well with insider threats that have no signatures. Constructivist learning theories are problematic because they assume new information builds on extant knowledge. This is problematic because many observable behaviors do not always have the same meaning when judgments are predicated on subjective knowledge. Cognitivist learning theories are appropriate for insider threat analysis research because they deal with how people solve problems (Mandler, 2002). ITA requires analysts to identify behaviors and make inferences to a cause. The theory of attribution is an applicable cognitive learning model because it deals with the reasoning of cause and effect.

1. Attribution Theory

Attribution theory is an artifact of cognitive psychology that is concerned with how people assign causal explanations for certain events (Harvey, Madison, Martinko, Crook, & Crook, 2014). Attribution theory posits that people will attribute behavior to either internal or external factors based on observations. Behavior attributed to internal cause assumes the behavior is under personal control; otherwise the behavior is attributable to some external cause. Fritz Heider's (1958) seminal work on attribution theory suggests that people act as naïve psychologists as they search for the reason certain events occur. Attribution theory is widely applied to educational contexts (Weiner, 1972), marketing (Laczniak, DeCarlo, & Ramaswami, 2001), and recently to insider threats (Posey, Bennett, & Roberts, 2011). This research applies attribution theory to analysts who seek out insider threats.

People have an innate drive to give causal explanations. According to Hiedler, "attribution is part of our cognition of the environment. Whenever you cognize your environment you will find attribution occurring" (Harvey, 1984, p. 428). Attribution theories examine how people gather, combine, and perceive information to make causal judgments (Fiske & Taylor, 1991). Perhaps the most popular, well-established attribution theory that focuses on how the perceiver attributes cause to an actor's behavior is Harold Kelley's (1973) covariation model.

Kelley's covariation model explains how social perceptions are used to make attributions for observed behaviors. The model is well suited for ITA because it is indifferent to intent. According to Kelley's model, factors that influence attributions to either internal or external causes include consensus, consistency, and distinctiveness. The consensus element explores why a person's behavior may deviate from the behaviors of others in the same situation—when consensus is high, people tend to attribute a behavior to some external cause. Consistency relates to how consistent a behavior is for the specific situation over time; when consistency is high, people tend to relate the anomalous behavior to some internal cause. Distinctiveness questions if the behavior is distinct among similar situations. When distinctiveness is high, people also tend to attribute a behavior to an internal cause. How each of the factors co-vary predicts

whether people attribute anomalous behavior to an internal or external cause. Kelley's model loosely relates to Baracaldo and Joshi's (2013, p. 237) precursors known to insider threats. Anomalous behavior attributed to an external cause may exonerate a suspect, while attribution to an internal cause may implicate insider threats.

According to Kelley and Michela (1980, p. 471), people use past subjective judgment to determine if there are "multiple sufficient causes" or "multiple necessary causes." The difference is analogous to "OR" and "AND" Boolean operations. In the case of multiple sufficient causes (AND operation), several authors stress the significance of schemata in causal attributions (Griffiths & Tenenbaum, 2009; Oliveria, 2007; Kelley, 1973; Thorndyke & Hayes-Roth, 1979). Kelly and Michela (1980, p. 471) defined a causal schema as "a description of the common person's conception of how two or more causes combine to produce a certain effect." As schemata interact with multiple behaviors, people must accommodate multiple schemata simultaneously to assign attribution to a set of behaviors. This implies that additional cognitive resources are necessary to accommodate the need to make attributions. Oliveira (2007, p. 13) theorized "once schemata is formed there will be a resistance to change." A reasonable explanation for the "resistance to change" is that schemata changes increase cognitive load when people confirm or reassign attributions as they reconcile new information.

2. Cognitive Load Theory

A major challenge to insider threat analysis is overcoming information overload (Cappelli et al., 2012, p. 196; Garst & Gross, 1997). The first recorded conceptualization of information overload may be credited to King Solomon, who 3,000 years ago warned that the making and studying of books is endless and will eventually weary the body. He concluded that wisdom can be summed up as "fear God and keep his commandments." Clearly, the conceptualization of information overload is not new.

There are known limitations to human information processing capacity (Simon, 1996). Cognitive performance is known to decrease when information processing demand exceeds the capacity to process it (Sweller, 1988). Information overload is a phenomenon that occurs when the demand for information processing exceeds that

capacity primarily due to processing time constraints (Schick, Gordon, & Haka, 1990). A body of research in the 1990s named the phenomenon, including Shenk's "data smog" (1997, p. 31) and "information-fatigue syndrome" (Oppenheim, 1997, p. 246). The academic literature explains it in terms of several factors that collectively limit the capacity to accommodate information-processing demand (Eppler & Mengis, 2004; Jackson & Farzaneh, 2012). Well-established research agrees that there is an optimal balance between information-overload factors and decision-making performance (Miller, 1995; Schroder, Driver, & Streufert, 1967).

Meadow and Yuan (1997, p. 701) point out that data refers to a "set of symbols with little or no meaning to a recipient" and information to a "set of symbols that does have meaning or significance to the recipient." According to Meadow and Yuan, data has the potential to be information, but may not be perceived as such. For instance, an unwitting threat analyst may look through pages of sensor feeds and extract little information, but a focused analyst may be overwhelmed with information because he is able to "see" more in the data.⁶ The literature also suggests that after the optimal point is exceeded, information-processing capacity will dramatically decrease (Miller, 1956; Griffeth, 1998). Starbuck and Milliken (1988) found that sense-making under conditions of low awareness contributes to information processing limitations.

a. Information Overload

There are competing precepts of load as an information measure. One conceptualization is the number of cues (Chewing & Harrell, 1990) or chunks (Simon, 1996, p. 81) presented and subsequently used for decision making. Working, immediate memory is generally limited to seven chunks, give or take two (Miller, 1956). The alternative conceptualization is similar, but defined by time limitations. Farace et al. (1977, p. 103) express information in common units called "messages" and conceptualized load as a rate. In this sense, information overload occurs when the number of messages within a certain period exceeds information-processing capacity (Schick et al., 1990). This

⁶ I use "sensor feeds" as a generalization for any packet captures, web logs, access logs, or other machine-generated data.

alternative view holds that an individual who has the required time available to process information is not overloaded. The two information-load conceptualizations are the same, with the exception of time as a component factor. Farace and Schick's definition represents continuous decision-making operations and Simon's is momentary.

The literature articulates several factors that contribute to information overload (Jackson & Farzeneh, 2012). These can be divided among properties of the environment (Eppler & Mengis, 2004), the individual (Haasse et al., 2014), and information complexity (Klausegger, Sinkovics, Zou, & Joy, 2007). This research focuses on the relationship between the individual and the information complexity—specifically, information sources (Edmunds & Morris, 2000). Measures for information overload are not new; previously validated surveys measured the perception of information overload in prior published studies (Karr-Wisniewski & Lu, 2010).

b. Information Sources

Humans generally make decisions under constrained time, knowledge, and information-processing capacity (Gigerenzer, 2001). As a result, information sources are beneficial up to some optimal point, after which additional sources become a burden (Klein, Moon, & Hoffman, 2006). A widely held explanation from cognitive load theory posits that information-processing capacity is limited by an individual's working memory (Sweller, 1988). As a result, people tend to prune all but the most useful information sources (Savolainen, 2007).

Following Herbert Simon's (2000) bounded rationality concept, Karr-Wisniewski and Lu (2010) suggest that information pruning will happen when information-processing capacity is exceeded, a process that differs from first determining which information sources are most useful. Recall that threat analysts must query all sources because, unlike investigators, they do not know which source is most useful *a priori*. Savolainen (2015, p. 619) offers that people generally use a "withdrawal strategy" to keep information sources to a minimum in order to prevent information overload *a priori*. There is substantial research on the factors that contribute to information overload (Eppler & Mengis, 2004), but there is yet no empirical test of the number of references as an

independent factor. Jackson and Farzaneh's (2012, p. 531) theory-based model of information overload includes information sources as a factor, but they assert that additional research is needed to determine the "values and accuracy" of the factors.

There are multiple concepts of an information source as a factor of information overload. Wu (2005) distinguishes between electronic and print resources. Bawden and Robison (2008) add that resources are available in an overwhelming number of media and formats. Dempsey (2008) states that a source is an entry point into an information network. Burns and Bossaller (2012) suggest that sources can be the communication technology used to access information. It follows that an information source is distinguished by mode of transmission, format, technology, and access.

The research on information overload agrees that too much information will do more harm than help. This view holds that there is some optimal load point at which all other points are suboptimal, assuming that information underload is also detrimental. Following the time-agnostic view of information load, this dissertation conceptualizes the lack of relevant information as ignorance. In this sense, information load is conceptualized inversely, whereby an analyst who has all the available information required for solving a problem lacks ignorance and one with no information available to solve a problem (including information that there is a problem) is fundamentally ignorant.

3. The Taxonomy of Ignorance

It is difficult to make causal attributions when information is missing and if we do not know what is normal, it is hard to identify what is anomalous. Theories of causal induction posit that prior knowledge informs causal inference (Griffiths & Tenenbaum, 2009). It stands to reason that ignorance can affect how people make attributions, especially when multiple people with diverse experiences are involved in making attributions. Samuel Holtzman (1989) categorized the lack of information available for decision making, or ignorance, into seven qualitatively distinct levels. The two highest levels represent problems that allow monotonic reasoning and the remaining levels require non-monotonic reasoning; a form of reasoning for which conclusions can be invalidated with new information (McCarthy, 1986)

The nature of loosely circumscribed problems requires convergence at a deeper level of ignorance than one must accommodate for a highly circumscribed problem. That is to say, as ignorance decreases, a problem becomes more circumscribed. Holtzman's (1989, p. 27) taxonomy of ignorance levels each require different ways of thinking in order to solve the type of problem each level represents. There is little progress toward this understanding of ignorance with the exception of Denby and Gammack's (1999) models of ignorance for decision support systems. Though not perfect, the taxonomy presents seven levels of ignorance that *ipso facto* represent different problem types. Table 2 presents the taxonomy of ignorance.

Table 2. Taxonomy of Ignorance. Source: Denby & Gammack (1999).

Ignorance Level	Description	Knowledge Required
Combinatorial	Computational task too difficult, e.g., problem with 10^{40} variables.	Mathematics model available; use of supercomputers.
Watsonian	Cannot make the connection from all the clues; solution method incomplete.	Method for determining the important facts from the unimportant ones, and drawing the right conclusion.
Gordian	King Gordius tied a knot for the future king of Asia to untie. Alexander the Great was able to "untie it" by cutting the knot with his sword, thus solving the problem in an unusual way.	Lateral thinking—are there "rules" to be broken?
Ptolemaic	Attributed to the Greek Mathematician and astronomer, Ptolemy, whose model of the universe centered around a stationary earth.	Evidence and observation of reality.
Magical	"No one knows how it works, but everyone knows that it works," e.g., the use of Aspirin and other similar drugs.	Trial and error.
Dark	No model is available but one is aware of the issues, e.g., "What is Life?," "Consciousness," etc.	Future of science.
Fundamental	Unaware of issue. (Ignorance is bliss!)	

It appears Holtzman would affirm that ITA proceeds from at least a Gordian level because ITA is closely related to the circumscription problem. Circumscription problems are known to involve non-monotonic reasoning. Insider agents continuously produce information, so ITA appears to be non-monotonic process. However, analysts must make decisions based only on the information available during a single inference cycle. Inference cycles are essentially recognize–act events based on the available information at a specific moment, so the reasoning involved appears monotonic (Meadows, Langley, & Emry, 2014).

Holtzman’s taxonomy does not explain how much one level differs from another. Also, combinatorial ignorance is not so much a problem of ignorance as it is a lack of information-processing capacity. Ptolemaic ignorance, from Ptolemy’s astronomical model, assumes there are multiple explanations to account for the same observations. In the case of Ptolemy’s ingenious geocentric model of the solar system, the data, model, observation, and predictions all fit. As did the Copernican model, which was simpler, yet both models were the product of the same level of ignorance. Ptolemaic ignorance is better classified within the philosophic principle of Ockham’s razor. Problem solving under conditions of fundamental ignorance is not testable in a laboratory because the very knowledge of the problem reduces the ignorance level.

The remaining ignorance levels (Watsonian, Gordian, magical, and dark) can be quantitatively specified in a more parsimonious taxonomy. Watsonian ignorance, from Sherlock Holmes’ famous “elementary, my dear Watson,” represents a problem with all the information necessary to deduce a solution; one need only solve the problem. Gordian ignorance derives its name from King Gordias’ legendary knot left for the future ruler of Asia to untie. Alexander the Great drew his sword and cut the knot. In this case, Alexander knew the end result and he subjectively bounded the problem so he could solve it. Magical ignorance takes its name from knowing something is so, but not knowing how it is so. In other words, magical ignorance allows knowledge that a problem has a solution, but not what the solution is. Those with magical ignorance must pick the best of solution possibilities informed only by existing knowledge. Dark ignorance is simply an awareness of the problem with no other information. Dark

ignorance includes ignorance of the possibility of a solution such that one must look at how problem components are interrelated to determine if any solution is feasible. A proposed refinement of Holtzman's taxonomy is presented in Table 3.

Table 3. Proposed Taxonomy of Ignorance Refinement.

Ignorance Level	Knowledge Allocation	Knowledge Required
Watsonian (1)	Problem, expected end result, bounds of the problem.	Solution
Gordian (2)	Problem, expected end result, and no bounds to the problem.	Problem space + Solution
Magical (3)	Problem, knows there is an end result but not what it is, and no bounds to the problem.	Recognition + Problem space + Solution
Dark (4)	Problem, does not know if there is a solution to the problem, and no bounds to the problem.	Inter-relationships + Recognition + Problem space + Solution

ITA problems are both monotonic and loosely circumscribed at the instant of a single inference cycle. Dark, magical, and Gordian ignorance levels are not solved by obtaining more information such that the solution is clear. Doing so would decrease the ignorance level of the problem until the problem becomes a well-circumscribed Watsonian problem. Rather, if one *were* to solve a problem at deeper than Watsonian ignorance, he must reason through possibilities that seem to present a feasible solution and select the best one at that time. Thus, I infer that ignorance is relatively low under Watsonian conditions.

Detectives investigate known infractions and identify a suspect by establishing means, motive, and opportunity (Swanson, Chamelin, Territo, & Taylor, 1992). Insider threat analysts have no such luxury. They do not know if an infraction was committed or malevolent insiders are present, so they must infer that a sequence of events is best

explained by a latent insider threat (Ard, Bishop, Gates, & Sun, 2013). These factors explain why ITA differs from investigation and requires an alternative way of thinking (Borum, Fein, Vossekuil, & Berglund, 1999).

McCarthy's (1980) circumscription concept described a loosely circumscribed problem in a formal decision system. McCarthy reasoned a qualification problem from sentences of logic. For instance, one can go into infinite regress when qualifying what it takes to make a boat float, but it is relatively simple to assume a boat floats unless something explicitly prevents it. Little has changed over the last 30 years, and the circumscription problem persists in the cybersecurity domain. Computers are partially capable of bounding circumscription problems through a pseudo-cognitive approach with expressly defined processes modeled off of humans (Kelly, 2014; Oltramari, Ben-Asher, Cranor, Bauer, & Cristin, 2014). Human minds naturally handle these problems because human reasoning can make assumptions from experiences that relate to a particular observation.

Ignorance effects are intuitive and implied by extant literature; the question lies in considering how well humans fill in the gaps to overcome ignorance when making causal attributions. For instance, Holtzman (1989) described the famous geocentric astronomical model that Ptolemy presented to explain the motion of the heavenly bodies. Ptolemy's model convincingly solved the problem, but his model was incorrect. Insider threat analysts similarly make attributions by accommodating ignorance with convincing explanations. McCarthy's (1980) circumscription principle posits that unavailable information may change a decision if made available. A contemporary perspective would ask, "Does ignorance cause incorrect insider threat assessments?" An acceptable answer to this question leads to the first hypothesis for empirical testing:

Hypothesis 1: A higher level of ignorance will cause lower analyst accuracy.

4. ITA References

The effects of ignorance emerge from a lack of information just as the effects of overload emerge when the information resources available do more to hinder than aid. Reichardt (2006, p. 105) introduces "reference overload" as a term from library science,

viewing information overload from the perspective of the information giver, in a library context. According to Reichardt, reference overload occurs when a library presents too many relevant information sources to a patron. The patron views this as information overload, while “librarians could consider it ‘reference overload’” (p. 106). He distinguishes reference overload from information overload because patrons are not information overloaded when reference overloaded—rather, it is the opposite. A possible mitigation is to “try to find the balance between listing too many versus not enough resources” (p. 108).

Insider threat analysts are known to use information from a number of references (Faber, 2015). There are at least 11 documented ITA references, including human resources (HR), security audit (SA), counterintelligence (CI), and social intelligence (SI) (Guido & Brooks, 2013; Maybury et al., 2005; Brackney & Anderson, 2004). Kelly and Anderson (2016) acknowledge that some agencies use more references than others, but offer no evidence that more references over a baseline capability affects analyst accuracy or promptitude.

The law of diminishing marginal returns is an economic principal stating that when a resource is increased and all else is equal, the resulting benefit will eventually diminish (Samuelson & Nordhaus, 2001). This law is called the “marginal-productivity idea” in information science (Iselin, 1988). The marginal-productivity concept basically confirms that increasing the number of references will provide relatively less additional information. A common example is social-networking services. Myspace was once the only prevalent online social-networking information source; if a user had a social-networking presence in 2003, chances are it was limited to Myspace alone. Today, a user may have a profile on Myspace, Facebook, LinkedIn, Snapchat, Tinder, Twitter, eHarmony, and Yelp, among others. Profiling an individual based on his social-network presence requires a different amount of effort today, but the benefit of processing seven profiles is not necessarily seven times greater than one. This is consistent with current research that suggests providing more information does not necessarily result in better crime prediction (Jackson, 2014; Levin, Bean, & Martin-Browne, 2012) and may prevent proper analysis (Sanders et al., 2014, p. 439). This implies that references must not

provide irrelevant or duplicate information, but must offer additional perspectives to be useful.

The UST multiple perspectives approach (Mitroff & Linstone, 1993, p. 99) as a framework for reference selection loosely relates to the multiple factors described in Kelley's (1973) covariation model. Both the UST model and the covariation model describe organizational and personal perspectives that together provide more meaning than either individually. References that support multiple perspectives are important because insider threat analysts require a synthesis of information from various references to perform their duties (Greitzer & Ferryman, 2013; Cappelli et al., 2012). Additional references help to give patterns meaning (Libicki & Pfleeger, 2004) and decision-making performance generally improves when more relevant information is available (Manis, Fichman, & Platt, 1978).

Anecdotal law enforcement information-sharing success stories perpetuate the idea that the availability of more references enables predicting and preventing crime (Executive Order No. 11587, 2011), and that in some cases references did not directly contribute to a thwarted attack (e.g., *U.S. v. Shahzad*, 2010). Since the 9/11 World Trade Center attack, the movement to increase references via information sharing has become a central security focus, as reflected in two national strategies (White House, 2007; White House, 2012). In line with these strategies, the Department of Defense (DOD) implemented a policy that requires the integration and synchronization of programs across the DOD, through a capability that involves diverse specializations and communities (DOD, 2014). Coincidentally, multibillion-dollar outlays for fusion centers that bring together nearly every law enforcement–related specialty and reference under the sun have become the *sine qua non* in preventing crime (Government Accountability Office, 2010). Persistent questions about the value of such efforts remain unanswered (Davies & Plotkin, 2005, p. 62). Notwithstanding substantial outlays in personnel and technology, however, there remains little to show for these investments (Permanent Select Committee on Investigations, 2012, p. 9).

The substantial increase of information available for threat assessments may have a related overload effect. There are two concepts of information overload that confuse the

meaning of Garst and Gross's work. One is a time-centered view that suggests an analyst will experience information overload under time constraints (Schick et al., 1990). The other centers on memory, suggesting that an analyst will experience information overload when the number of cues exceeds the limitations of working memory (Simon, 1996, p. 81). These concepts create ambiguity—do too many cues or too high a rate of information present a problem? If it is too many cues, then decreasing the number of references may be an appropriate strategy to mitigate information overload. If rate (i.e., too little time allotted), then simply increasing the number of insider threat analysts to process the information may best mitigate overload. Following the theory of constraint, more information should increase the time required to process the information. Such postulates lead to my second and third hypotheses:

Hypothesis 2: A lower level of ignorance will cause higher analyst time.

Hypothesis 3: A higher level of ignorance will cause lower analyst confidence.

According to organization theory, organizational structure can affect human information processing performance (Lenz, 1981). I argue that organizational structure and ignorance create specific effects and may affect analyst accuracy and time, and could interactively affect perceptions of information overload. An empirical test of ITA with people organized in teams or as individuals to see how structure interacts with various information constraints may take us a step closer to understanding why large investments in ITA programs appear to have little effect on analyst performance.

C. ORGANIZATIONAL THEORY

In classical organizational theory, an organization is a social artifact “set up to do something” (Porter, Lawler, & Hackman, 1975, p. 69). The contingency theory of organizational design is that “there is no one best way to organize” and “not all ways to organize are equally effective” (Galbraith, 1977, p. 28; Thompson, 1967, p. 78). Some organizational theories hold that organizations employ people to accomplish a shared task “through division of labor” (Galbraith, 1977, p. 3); others state that organizations do so as “coordinated activity systems” (Daft, 2007, p. 10). Organizations generally receive inputs and, through some interdependent relationship, produce outputs to accomplish a common

goal (Farace, Monge, & Russell, 1977). These descriptions imply that an organization consists of individuals in a group who, with or without division of labor, accomplish a common goal.

1. Organizations as Information Processors

Classical theories of organizational management tend to view organizations as output-oriented producers (Simon, 1973).⁷ Simon cites Peter Drucker's conceptualization of the post-industrial society as a contemporary view of organizational information processing. According to Simon (1973), many modern organizations focus on how best to make decisions rather than simply on producing widgets—that is, they process information. This theory of organizations as information processors is consistent among several well-established organizational theorists (Galbraith, 1974; Tushman & Nadler, 1978; Levitt et al., 1999). Information-processing organizations are limited to the constraints experienced by all output-oriented organizations. Specifically, the individual producer, whether machine or human, has a limited capacity for information processing work. As a result, information-processing organizations tend to use division of labor to share information-processing tasks.

Applying a contingency-theoretic lens applied to information-processing organizations implies that there are multiple ways for organizations to process information, and some ways may be better than others. According to Klausegger et al. (2007), organizational design may play a significant role in information overload. Specifically, the disintermediation that occurs as a result of removing steps between the information and the consumer (Sarkar, Butler, & Steinfield, 1995) reduces the overall encumbrance within a communicating system. Division of labor compels disintermediation in information-processing organizations, but allows greater information-processing capacity (Cukrowski & Baniak, 1999).

Tushman and Nadler (1978) focused on task complexity and task interdependency as factors to consider when determining the proper fit between environmental constraints and information-processing demands, arguing that effectiveness is associated with the fit

⁷ See Wren (2005) for a review of classical organizational-management theory.

between the demands and the capacity available to process information. Further research on information underload agrees with Tushman and Nadler's contingency theory (O'Reilly, 1980; Griffeth, Carson, & Marin, 1988). Drawing from O'Reilly (1980), performance in information-processing organizations, unlike material-processing organizations, may also be degraded by underload conditions. Tushman & Nadler's optimization problem for information-processing organizations is shown in Table 4, indicating that the contingency theory in information-processing organizations is a classic optimization problem.

Table 4. Information Processing Contingency Matrix.
Source: Tushman and Nadler (1978, p. 619).

		Information processing capacity	
		High	Low
Information processing requirements	High	Match	Mismatch
	Low	Mismatch	Match

Contemporary organizational-contingency theory offers an ontology of organizational configurations and coordination systems theorized to optimally accommodate various constraints. Mintzberg (1980) posits that organizations can be structured as machine bureaucracies, professional bureaucracies, adhocracies, simple structures, or divisionalized forms to accommodate environmental uncertainty, control, and expertise demands and conditions. Each configuration represents a structure that integrates subunits into a greater whole. Information-processing organizations, regardless of structure, must make decisions based and built on the interpretations of the lowest subunit—the personnel who interpret data.

Interpretation is a waypoint between data and information, requiring a human mind when contextual relevance is prone to change. Assuming Heraclitus is correct that change is certain, computers are incapable of interpretation under conditions of dynamic

contextual relevance because computers programmatically follow rules (Dreyfus & Dreyfus, 1986). To the extent that contextualization is an interpretative activity, it is closely related to Weick's (2005) conceptualization of sense-making.

Contextualization is basically a human sense-making activity, as stimuli are organized into a framework (Weick, 1995, p. 4) that allows a person to "comprehend, understand, explain, attribute, extrapolate, and predict" (Starbuck & Milliken, 1988, p. 51). Starbuck and Milliken (1988) found that sense-making under conditions of low awareness contributes to information-processing limitations. The literature, however, tends to describe sense-making as an organizational-learning process required for "consensually constructed, coordinated system of action" (Taylor & Van Every, 2000, p. 275). The dynamic interactions between sense-making elements create knowledge (Nonaka, Toyama, & Nagata, 2000). Nonaka et al. (2000) assert that context necessarily precedes knowledge. Without proper context, a view cannot be communally justified as a true belief because differing predicate knowledge applies (Hesse, 1970; Hanson, 1958). This implies that intermediation exists between individual and team sense-making. I infer that the same is true of individual and team contextualization. Thus, intermediation is a result of division of labor in an information-processing task that includes contextualization.

Media synchronicity theory describes a similar phenomenon within a group information exchange. According to Dennis, Fuller, and Valacich (2008), communication has a convergence dimension in addition to conveyance. The theory provides that communication requires both dimensions, conveyance and convergence, for successful completion of any task that involves more than one individual. Media synchronicity theory concludes that media fit for a communication task affects communication performance and face-to-face is the best medium for convergence.

Division of labor requires eventual reassembly. Similarly, reassembly logically compels interdependence among subunits. Thompson (1967) presents three types of interdependence that accommodate reassembly, contingent on increasingly complex organizational structures. Pooled interdependence is described by Thompson (1967, p. 54): "Each part renders a discrete contribution to the whole and each is supported by

the whole.” Sequential interdependence includes pooled interdependence and takes a serial form, such that the output of a preceding subunit becomes the input of a subsequent subunit, in the manner of an assembly line. Reciprocal interdependence includes sequential interdependence, but the output of the subsequent subunit becomes the input of the preceding subunit. This research evaluates the effect of information processing under conditions of reciprocal interdependence against that of non-interdependent information processing. The two conditions of interdependence fit the descriptions of the two insider threat–mitigation organization designs presented by Kelly and Anderson (2016).

Groups generally perform better than individuals at complex tasks (Kerr & Tindale, 2004). Related research suggests that group decision making is better than an individual’s (Brodbeck, Kerschreiter, Mojzisch, & Schultz-Hardt, 2007). Antecedent research demonstrates that a judgment from each of 50 people is equal to 50 judgments from one person (Farnsworth & Williams, 1936). Mao, Mason, Suri, and Watts (2016) find that teams outperform independent workers at complex tasks. Related research tends to be consistent in other domains (Nielsen, 2011; Cheung & Palan, 2012; Kerr & Tindale, 2004). Theories of specialization and process loss may explain why large, well-funded programs leveraging ITA teams have not resulted in decisively better analyst performance; but no conclusive evidence yet exists in the academic literature. This debate requires empirical testing to confirm or refute these postulates as reflected in the fourth hypothesis:

Hypothesis 4: Teamwork will cause higher analyst accuracy than individual work.

2. Specialization Theory

Specialization theory was first documented in a dialogue between Socrates and Adeimantus in Plato’s *Republic*. Socrates reasoned that men are best served by specializing in the production of certain things and trading those things according to need. Otherwise, each man must alone produce everything he needs. Adam Smith expanded on division of labor (or specialization) in his *Inquiry into the Wealth of Nations*. Smith’s theory of specialization holds that a group of persons who are

specialized for subcomponents of a complex task is more efficient than a group comprising the same number of people who individually perform the same task.

Specialization is understood as an advanced form of division of labor that allows the worker to become more skilled at a certain task (Heath & Staudenmayer, 2000). In classic organizational theory, specialization is “the degree to which tasks are subdivided into separate jobs” (Daft, 2001, p. 10). I interpret this to mean that each separate job requires a separate individual to fill the role. Organizations typically create a division of labor to overcome the limited information-processing capacity of individuals (Simon, 1962). In this scheme, workers are specialized to perform a smaller task that is within the limitations of individual information-processing capacity. Specialization hypothetically overcomes the cognitive and knowledge limitations of human beings, but simultaneously increases interdependence between work roles (Galbraith, 1977, p. 13; March & Simon, 1958, p. 159).

A team is generally defined as a group of people working together to perform a common task. The role of specialization among teams carries sufficient importance such that a team is sometimes defined as a group of cooperative workers that produces something specifically by performing different tasks and functions (Becker & Murphy, 1994). A specialized team is characterized by interdependence among work roles that draws on explicit knowledge, and a team with no specialization is characterized by the consolidation of work roles that draw on implicit knowledge (Farace, 1977, p. 20). Regardless of specialization, the terms “team” and “group” are generally interchangeable under the condition that individual members collectively perform a common task.

Current research suggests that specialized teams perform better at highly circumscribed tasks, but there is little literature on the effects of specialization on loosely circumscribed tasks that introduce confounding complexities (e.g., ITA; Mao, Mason, Suri, & Watts, 2016). For instance, Staats et al. (2012) mention studies employing LEGOs to test specialization theory, but LEGO problems, regardless of complexity, are bounded by number and shape and generally have a known solution (e.g., LEGO set 10188, “Death Star”). The exception to Mao et al.’s observation are experiments related to Nielsen’s (2011) conceptualization of micro-expertise in crowdsourcing, but micro-

expertise by definition presupposes that someone in a large crowd already knows a solution to a particular problem.

In a rare test of teamwork on a loosely circumscribed problem, Mao et al. (2016) assigned teams of various sizes to a loosely circumscribed task and found that performance increases with team size. Mao et al. tasked groups with analyzing 1,567 tweets to determine areas of crisis. The results were benchmarked against a gold standard provided by experts to determine group performance. Unfortunately, the number of tweets was not proportional to the persons in the group, resulting in an information load that was suitable for large groups, but overloaded smaller. Had Mao et al. equally distributed the information load per individual; it is likely the results would have been more consistent with the findings of prevailing research.

A natural consequence of specialization is the need for integration; in other words, specialization breaks a task into narrowly defined roles that compel an eventual reassembly (Thompson, 1967, p. 75). Information-intensive tasks can cause problems with integration because specialized knowledge is hard to interpret when it is not received in the same context in which it was sent (Heath & Staudenmayer, 2000). An information barrier may arise between specialists who perceive the world from different viewpoints, probably impeding knowledge integration. Additionally, people generally overestimate how well they communicate knowledge to others. Newton (1990) empirically demonstrated the phenomenon by having some test participants tap the rhythm of 25 well-known songs, and having other participants attempt to identify the song by listening to the taps. Half of the tappers predicted that the listeners would identify the songs, but only 2.5% of the listeners could correctly identify any of the common songs. Related research demonstrates similar findings in the tone of text messages (Keysar, 1994). This implies that the interdependence compelled by specialization can have a restrictive effect on a team's integrative capacity. Large information-processing tasks tend to require increased specialization (Drucker, 1988, p. 47), at least to some optimal point that, once surpassed, may result in negative consequences (Hammer & Champy, 1993, p. 51).

3. Process Loss Theory

It is safe to assume that people act differently when in the company of others, and that is the premise behind Bibb Latane's social impact theory. According to Latane (1981, p. 343), social impact is any change in the "physiological states and subjective feelings, motives and emotions, cognitions and beliefs, values and behavior, that occur in an individual, human or animal, as a result of the real, implied, or imagined presence or actions of other individuals." A popular example is provided by Solomon Asch (1951), who found that individuals are likely to submit an obviously erroneous response to a stimulus in order to conform to an incorrect majority. Latane was involved in several subsequent experiments that verified this effect in a number of social situations (Latane & Darley, 1970; Latane & Dabbs, 1975; Freeman, Walker, Borden, & Latane, 1975; Latane, Williams, & Harkins, 1979). Latane offers a general theory of social impact that describes social force as a function of strength, immediacy, and number of persons present.⁸ This implies that, *ceteris paribus*, teams will perform differently from individuals and team performance may be affected by group size. Survey instruments that measure social impact have been validated in prior research (Mulvey & Klein, 1998).

An intuitive linear relationship exists between number of workers and capacity for work. For instance, one horse provides one horsepower; two horses provide two horsepower, or double the energy of a single horse. However, a large body of research suggests that team performance has a curvilinear relationship with team size and at some point may exhibit a negative relationship. The counterintuitive relationship between team size and performance is known as the Ringelmann effect, named after experiments in the early 20th century by German psychologist Maximilien Ringelmann.

Ringelmann demonstrates that productivity per individual worker decreases as team size increases for simple tasks such as rope pulling and milling flour. According to Ringelmann, "When several sources of motive force work simultaneously on the same thing, the utilizable force of each is less, with the same fatigue, than if the sources of

⁸ According to Latane (1981), strength is the salience of those in the group (generally determined by age or status) and immediacy is determined by proximity in space or time and absence of some intervening barrier.

motive power function separately” (1913, p. 19). Ringelmann observes the effect by varying the number of workers turning a flour-mill capstan. When additional workers are added to the capstan, at some point individuals may tread the capstan without adding pressure, and even allow the capstan harness to tug them, increasing the work for other team members performing the same task (Kravitz & Martin, 1986). Ringelmann’s (1913) empirical findings followed a similar experiment that involved pulling a rope, in which he observed individual and total forces on the rope using a recording dynamometer. The results shown in Table 5 indicate a negative relationship between team size and individual performance.

Table 5. Relative Performance as a Function of Group Size.
Source: Ringelmann (1913, p. 9).

# of Workers	Furnished per worker	Total
1	1.00	1.00
2	0.93	1.86
3	0.85	2.55
4	0.77	3.08
5	0.70	3.50
6	0.63	3.78
7	0.56	3.92
8	0.49	3.92

Ringelmann’s work was not published in his time, but many subsequent scientific contributions have verified and explained this phenomenon under various conditions of task complexity—notably, Ivan Steiner’s (1966) paper on process loss theory.

Steiner's process loss theory offers several explanations for the Ringelmann effect, based on organization contingency. Steiner identifies five models that can explain the productivity of a group; the four that best explain process losses are discussed here (Steiner, 1972, ch. 2). The additive model addresses the relationship between group size and individual productivity loss as a function of "coordination links" between the team members contributing to a task. This model requires that all team members perform the exact same function, such as pulling a rope. The relationship Steiner discovered follows the principal of Metcalfe's law, which states that $n(n-1)/2$ is the number of communication links for n nodes. Thus, two workers require 1 link, 4 require 6, and 8 require 28 links. According to Steiner, these links are nearly proportional to the discrepancy between potential and actual productivity. The research suggests that those pulling the rope may have been unsynchronized in such a manner that sporadic tugs ultimately lowered performance.

Steiner's disjunctive model accounts for tasks in which productivity is determined by the performance of the most competent member. The effect is common to knowledge-industry professions like nursing, wherein a single expert in the operating room may save a life and the absence thereof may cost one (Benner, Tanner, & Chesla, 2009, p. 236). This phenomenon is what Benner calls "pooled expertise," a similar concept to Neilson's (2012, p. 26) "microexpertise." According to Neilson, as group numbers increase, so does the likelihood that someone in the group has a solution to a particular problem. Steiner cites Smith (1953, p. 572) for mathematical proof of pooled expertise.

According to Smith, a randomly selected group of four persons in a normal distribution will have the statistical likelihood of containing one person in each of the 20th, 40th, 60th, and 80th competency percentiles. Thus, the most competent person in a group is likely to be in the 80th percentile, and it follows that the most competent person in a seven-person group is likely to occupy the 87.5th percentile. Mathematically the larger the team size, the greater the odds of having a more highly competent member. However, process loss also increases, due to an increase in insignificant members—there are equal odds of a more incompetent person on the team.

Describing the opposite effect is the conjunctive model, in which team performance is measured by the performance of the weakest link, for example, in a human chain (Steiner, 1972). Cybersecurity is an example of a complex task in a conjunctive model because “cyber-security operators must achieve perfect defense to keep out intruders” (Bejtlich, 2013, p. 11). Imperfect defenses leave an organization vulnerable, and an attacker need only exploit a single vulnerability to harm the whole. Thus, in a conjunctive model, a team with four competent members may perform better than one with seven competent members and one incompetent.

Finally, classical division of labor is an example of Steiner’s complementary model. A complementary model assumes that no individual team member acting alone has the resources to complete a group task. Staats et al. (2012) support Steiner’s complementary model, demonstrating that a two-person team may outperform a four-person team in LEGO assembly. In a complementary model, process loss can occur any time someone on the team finishes a subtask before someone else.

Each of Steiner’s models has some process loss that may explain why individual productivity tends to decline as group size increases. There are, however, alternative explanations, including the phenomenon whereby “individuals expend less effort when working collectively than when working individually” (Karau & Williams, 1993, p. 681). Closely related literature tends to explain this phenomenon as a function of social loafing.

Social loafing is such a significant problem that some regard the practice as a “disease” (Latane et al., 1979, p. 831) and those who loaf as “deadbeats” (de Pillis, 2016, p. 273). Several experiments demonstrate a negative relationship between the number of persons assigned to a task and individual effort (Staats et al., 2012; Sorkin, Hays, & West, 2001; Harkins, Latane, & Williams, 1980). Both menial and cognitively stimulating tasks are degraded by the social-loafing phenomenon (Robbins, 1995). It can be hard to detect productivity loss due to an individual within a group on an additive task because the more diligent members of a team tend to compensate for the deficiency of loafers (Schippers, 2014). This implies that individual performance must be measured, and participants must know that they are individually evaluated, in controlling for social loafing. Ingham, Levinger, Graves, and Peckham (1974) ruled out coordination

difficulties as a cause of social loafing. Thus, social loafing and coordination are defined in this research as independent factors that may contribute to process loss in team tasks that require information processing.

The demand for coordination increases as interdependence increases (Katz-Navon, 2005) and intermediation compels increased coordination as information-processing requirements increase. It follows that an informational view of group process will place greater focus on coordination over mere cooperation (Grant, 1996). Coordination neglect theory (Heath & Staudenmayer, 2000) tends to explain coordination problems as related to a negative synergy in team performance on interdependent tasks. Heath and Staudenmayer (2000) found that inadequate communication and insufficient translation were two factors causing coordination neglect, and both arise from the fundamental process involved with the division of labor. According to Heath and Staudenmayer, inadequate communication is simply the absence of communication when communication is necessary, and inadequate communication may be rectified by integrating efforts on an ongoing basis. This implies that a team in constant communication working a truly complementary task will not suffer from coordination neglect under the condition that messages are fully understood.

Translation problems are persistent because even face-to-face, real-time communications cannot rectify a translation problem. Translation problems arise when people try to communicate but are biased by their own knowledge, such that the message received is not the message sent yet both speaker and listener mistakenly perceive that the communication was successful. This problem is what some researchers call the curse of knowledge (Heath & Heath, 2006; Rubio-Fernandez & Glucksberg, 2012). In a striking example of how specialization can affect communication, Hinds (1999) demonstrates that people tend to communicate less effectively as their expertise in a specialty increases. Experts may lose the ability to communicate with novices, even when they perceive themselves as communicating effectively or dumbing it down so novices can understand. Process loss theory describes counter-intuitive productivity impedance that this research seeks to test in the context of ITA with the fifth hypothesis:

Hypothesis 5: Teamwork will cause higher analyst time than individual work.

D. ITA PERFORMANCE MEASURES

No standard metric exists to evaluate the success of an ITA program in reducing insider threats (Greitzer & Ferryman, 2013); in fact, the Department of Homeland Security rated the ITA measurement problem second on the 2005 INFOSEC hard-problems list. Currently, federal ITA programs gauge success by benchmarking against each other (NITTF communication, Appendix A). I present a way forward by evaluating the literature for common performance themes and applying those themes to ITA analysis for an objective performance measure.

According to Jay Galbraith, an organizations' performance is measured by "the degree to which they seem to accomplish their objectives" (1977, p. 1). Performance metrics focus on effectiveness (Maizlish & Handler, 2005, p. 53) and are simple, expressed in time or money as a percentage (Jaquith, 2007, p. 25). Speier et al. (1999, p. 345) measure decision-making performance in terms of "decision accuracy and decision time." Recent research on process loss in group collaboration measured performance in terms of accuracy and time (Marler & Marett, 2013). Following extant research, I measure performance in terms of accuracy and time.

There are two competing concepts of analyst accuracy measurement. The prevalent measure is the number of insiders who were prevented from becoming insider threats. This measure, however, is not falsifiable or objectively verifiable, unless all insider threats truthfully admit to wanton or negligent threat behavior. Furthermore, an employee cannot be compelled to incriminate himself in discourse with his employers.⁹ Thus, the prevalent measure is only valid for a count of those who voluntarily identify themselves as insider threats. As a result, there has yet to be any standard objective ITA

⁹ According to the U.S. Supreme Court opinion in *Garrity v. New Jersey* (1967), no statements can be compelled under threat of termination. Furthermore, compelled statements cannot be used in a subsequent criminal investigation.

performance measure across federal agencies.¹⁰ A second measure is the number of reasonably warranted insider threat behavior cases referred to an investigative authority.

Kelly and Anderson (2016) found that an ITA investigation process requires an analyst to elevate a case to an investigation when threats are considered sufficiently significant. This implies that the more often analysts can correctly identify and elevate warranted cases within a given time, the higher the likelihood an insider threat will be discovered in that time. Organizations that are set up to process information generally focus on optimizations that allow the organization to properly process more information while consuming fewer resources and less time. I propose that, as insider threat analysts become more effective at identifying and elevating cases of concern; the organizational performance, in terms of promptitude and accuracy, will improve.

Expectancy theory suggests that incentives positively affect task performance granted no incentive can increase performance into the realm of the impossible (Bonner, Hastie, Sprinkle, & Young, 2000). Bonner and Sprinkle (2002, p. 303) offer guidance directly relevant to laboratory studies by pointing out that “researchers have been encouraged to employ incentives in experimental studies so that subjects are sufficiently motivated and participate in a meaningful fashion,” and go on to cite “numerous studies show[ing] that monetary incentives and assigned goals generally have additive effects on performance.” Bonner and Sprinkle conclude that assigned goals and monetary incentives have independent, positive effects on performance. Everett, Price, Bedell, and Telljohann (1997) point out that the positive effects of performance incentives also manifest in survey research, with a 50% increased survey return rate for incentivized survey returns. Consistent with these findings, Stolovitch, Clark, and Condly (2002, p. 2) specifically state, “To focus on and persist in working toward a goal: Tangible incentives increase performance by 27%.” This research leveraged performance incentives to reduce the likelihood of participants to guess during insider threat analysis. The research also introduced a confidence measure to capture any residual guessing effect.

¹⁰ See Appendix A; the correspondence with the National Insider Threat Task Force provides no objective measures for any federal insider threat program.

E. ANALYST CONFIDENCE

In reality, it is impossible to know how many insider threats analysts overlook as a percentage. Furthermore, a person must be in the act for an analyst to know for sure if an insider threat would have carried out an attack against his organization if not identified by an analyst. This problem poses a philosophical quandary for theory pertinent to ITA. Insider threat analysts operate knowing there are unknowns. They use available information to make inferences into unavailable information. As a result, they cannot be definitively sure about a threat assessment; they must rely on how confident they are that their threat assessment is correct. It follows that an insider threat analyst who elevates a case and is uncertain about his decision has done little more than make a random guess.

Classic organization theorists agree that information processing organizations reduce uncertainty by acquiring more information (Galbriath, 1973). Daft and Lengel's (1986) media richness theory expanded the classical view by delineating a distinction between uncertainty and equivocality. According to Weick (1979), information stimulus with multiple interpretations increases the equivocality of that information. As a result, additional information with high equivocality offers little in reduction of uncertainty. Media richness theory suggests that the information transmission medium must be capable of conveying meaning along with data so information is received in the proper context. Media synchronicity theory extended media richness theory into team dynamics (Dennis et al., 2008). The media theories strongly suggest negative confidence effects with increasing the number of people in a communicating system due to ambiguity that results from information distortion. This debate is ideal for empirical testing in an ITA context presented in hypothesis 6.

Hypothesis 6: Teamwork will cause higher analyst confidence than individual work.

Attribution theory predicts similar confidence behavior because "fewer noncommon effects resulted in more confidence and more extreme inferences about the actor" (Kelley & Michela, 1980, p. 462). Insider threat problems are non-absolute and a propensity for information equivocality may increase when more than one mind is involved in the same inference cycle. This phenomenon is not new; for instance, March

and Olsen (1976) assert that increasing the number of decision makers increases the length of the decision process. This implies that, given various amounts of information and an increase in the number of people who must generate an explanation for observations, it becomes more difficult to converge ideas into common explicit language. An interaction is reflected in hypothesis 7 implied by the social impact posited in hypothesis 8.

Hypothesis 7: Teamwork and ignorance will interactively affect perceptions of information overload.

Hypothesis 8: A lower level of ignorance will cause higher perceptions of social impact.

F. SUMMARY

This literature review presented salient research describing the theoretical concepts within the focus of this dissertation. The chapter introduced literature covering insider threats to cybersecurity and the concept of insider threat analysis. This overview identified information overload as a conceptual problem for analyst performance. I proposed reducing relevant information (operationalized as ignorance) and distributing information between teams of people (operationalized as teamwork) as methods to reduce information overload so that ITA analysts can perform better. The work draws inferences from attribution theory, a product of cognitive psychology, and process loss theory, a product of organization theory, that predict how variations in ignorance and teamwork may affect analyst performance, namely accuracy and time. Eight hypotheses emerged subject to empirical testing in a laboratory experiment:

- Hypothesis 1: A higher level of ignorance will cause lower analyst accuracy.
- Hypothesis 2: A lower level of ignorance will cause higher analyst time.
- Hypothesis 3: A higher level of ignorance will cause lower analyst confidence.
- Hypothesis 4: Teamwork will cause higher analyst accuracy than individual work.
- Hypothesis 5: Teamwork will cause higher analyst time than individual work.

- Hypothesis 6: Teamwork will cause higher analyst confidence than individual work.
- Hypothesis 7: Teamwork and ignorance will interactively affect perceptions of information overload.
- Hypothesis 8: A lower level of ignorance will cause higher perceptions of social impact.

III. EXPERIMENT DESIGN

Chapter I identified two conceptual strategies for overcoming information overload: reducing information, and distributing the information among more people to better accommodate the load. Theories of attribution and process loss covered in Chapter II introduced the theoretical implications for both concepts. This chapter approaches the two concepts as measurable constructs: ignorance and teamwork, respectively. The literature review defined performance as a concept of productivity within an amount of time, operationalized as ITA accuracy and ITA time. This chapter operationally defines each predictor, dependent, and blocking variable and relates the variables within a factorial research design.

The literature reviewed in Chapter II strongly suggests that ignorance and teamwork will affect ITA accuracy and time. This chapter presents a research design that provides an empirical test for the eight hypotheses which emerged from that review. The experiment assesses the theoretical implications of ignorance (operationalized as high and low) and teamwork (operationalized as horizontally specialized and none) within the context of ITA. This chapter also provides the rationale for the research design selection and laboratory experimentation.

This chapter outlines the experiment participant selection, enumerates the laboratory experiment procedure, presents survey instruments, and describes the web-based experiment apparatus. This section offers role based access control as a method of partitioning insider threat scenarios and references between test groups in order to electronically enforce variations of ignorance and teamwork. The chapter concludes with the rationale for laboratory experimentation.

A. EXPERIMENT METHODOLOGY

The academic literature strongly implies that ignorance and teamwork have dynamic performance effects. This experiment will evaluate the effects of ignorance and teamwork to determine if the theoretical constructs behave predictably in a realistic ITA application.

1. Research Design

The research variables fit well within a 2 x 2 factorial design. Ignorance is varied between two conditions: high and low. Teamwork is varied between two conditions: horizontally specialized and none. There are five dependent variables including accuracy, time, confidence, perception of information overload, and perception of social impact. The research design is presented as a two-by-two factorial analysis crosstab in Table 6.

Table 6. Research Design.

		Ignorance	
		Low	High
Teamwork	Horizontally Specialized	Accuracy Time Confidence Information overload Social impact	Accuracy Time Confidence Information overload Social impact
	None	Accuracy Time Confidence Information overload	Accuracy Time Confidence Information overload

2. Procedure

The experiment followed a standard procedure that took between thirty minutes and two hours to complete. Prior to the experiment, each participant received an informed consent document to satisfy the requirements of the institutional review board (IRB). The informed consent document explained the nature of the research and the task requirements. The IRB protocol is in Appendix C. The experiment commenced with an entrance survey that collected demographic data. ITA followed the entrance survey, and the experiment concluded with an exit survey that measured ITA accuracy, time,

performance, confidence, information overload—and for teams, the perception social impact. The experiment took place in a distraction-free location.

The experiment procedure for individuals was as follows:

1. Participant receives a website login ID and password, unique to their assignment in the experiment design.
2. Participant logs on to <http://www.kellyapparatus.com> and views a welcome message with experiment instructions.
3. Participant views an instruction video that explains how to maneuver the ITA apparatus.
4. Participant skims the adjudicative guidelines.
5. Participant completes the entrance survey.
6. Clock starts when the entrance survey “submit” button is pressed.
7. Participant receives the scenario stimulus.
8. Participant reviews the available references.
9. Participant performs a threat assessment of the insider’s behavior.
10. Participant creates an insider threat analysis case with a case management survey.
11. The clock stops when the case management survey is initiated.
12. Participant submits their insider threat assessment.
13. Participant completes the exit survey.

The experiment procedure for teams assigned high ignorance is as follows:

1. Each participant receives a separate website login ID and password, unique to their place in the experiment design.
2. Both participants log on to <http://www.kellyapparatus.com> and views a welcome message with experiment instructions.
3. Participants view an instruction video that explains how to maneuver the ITA apparatus.
4. Participants skim the adjudicative guidelines.
5. Participants each complete separate entrance surveys.
6. Clock starts when the entrance survey “submit” button is pressed.

7. Participants receives scenario stimuli numbered 1 and 2.
8. Participants 1 and 2 review the Scenario 1 stimulus.
9. Participant 1 reviews their own references.
10. Participant 2 informs Participant 1 of the information in Participant 2's references.
11. Participant 1 performs a threat assessment of the insider's behavior.
12. Participant 1 creates an insider threat analysis case with a case management survey.
13. Server records clock time as soon as the case management survey is initiated (this is the ITA end time for Participant 1).
14. Participant 1 submits their insider threat assessment.
15. Server records clock time as soon as the case management survey is submitted (this is the ITA start time for Participant 2).
16. Participants 1 and 2 review the Scenario 2 stimulus.
17. Participant 2 reviews their own reference.
18. Participant 1 informs Participant 2 of the information in Participant 1's references.
19. Participant 2 performs a threat assessment of the insider's behavior.
20. Participant 2 creates an insider threat analysis case.
21. Server records clock time as soon as the case management survey is initiated (this is the ITA end time for Participant 2).
22. Participant 2 submits their insider threat assessment.
23. Server records clock time as soon as the case management survey is submitted.
24. Participants 1 and 2 complete individual exit surveys.

The experiment procedure for teams assigned low ignorance is as follows:

1. Each participant receives a separate website login ID and password, unique to their place in the experiment design.
2. All participants log on to <http://www.kellyapparatus.com> and views a welcome message with experiment instructions.

3. Participants view an instruction video that explains how to maneuver the ITA apparatus.
4. Participants skim the adjudicative guidelines.
5. Participants each complete separate entrance surveys.
6. Clock starts when the entrance survey “submit” button is pressed (this is the ITA start time for Participant 1).
7. Participants receives scenario stimuli numbered 1, 2, 3, 4.
8. Participants 1, 2, 3, 4 review the Scenario 1 stimulus.
9. Participant 1 reviews their own references.
10. Participants 2, 3, 4 inform Participant 1 of the information in each of their individual references.
11. Participant 1 performs a threat assessment of the insider’s behavior.
12. Participant 1 creates an insider threat analysis case.
13. Server records clock time as soon as the case management survey is initiated (this is the ITA end time for Participant 1).
14. Participant 1 submits their insider threat assessment.
15. Server records clock time as soon as the case management survey is submitted (this is the ITA start time for Participant 2).
16. Participants 1, 2, 3, 4 review the Scenario 2 stimulus.
17. Participant 2 reviews their own reference.
18. Participants 1, 3, 4 inform Participant 2 of the information in each of their individual references.
19. Participant 2 performs a threat assessment of the insider’s behavior.
20. Participant 2 creates an insider threat analysis case.
21. Server records clock time as soon as the case management survey is initiated (this is the ITA end time for Participant 2).
22. Participant 2 submits their insider threat assessment.
23. Sever records clock time as soon as the case management survey is submitted (this is the ITA start time for Participant 3).
24. Participants 1, 2, 3, 4 review the Scenario 3 stimulus.

25. Participant 3 reviews their own reference.
26. Participants 1, 2, 4 inform Participant 3 of the information in their references.
27. Participant 3 performs a threat assessment of the insider's behavior.
28. Participant 3 creates an insider threat analysis case.
29. Server records clock time as soon as the case management survey is initiated (this is the ITA end time for Participant 3).
30. Participant 3 submits their insider threat assessment.
31. Server records clock time as soon as the case management survey is submitted (this is the ITA start time for Participant 4).
32. Participants 1, 2, 3, 4 review the Scenario 4 stimulus.
33. Participant 4 reviews their own reference.
34. Participants 1, 2, 3 inform Participant 4 of the information in each of their individual references.
35. Participant 4 performs a threat assessment of the insider's behavior.
36. Participant 4 creates an insider threat analysis case.
37. Server records clock time as soon as the case management survey is initiated (this is the ITA end time for Participant 4).
38. Participant 4 submits their insider threat assessment.
39. Server records clock time as soon as the case management survey is submitted.
40. Participants 1,2,3,4 complete individual exit surveys.

3. Experiment Apparatus

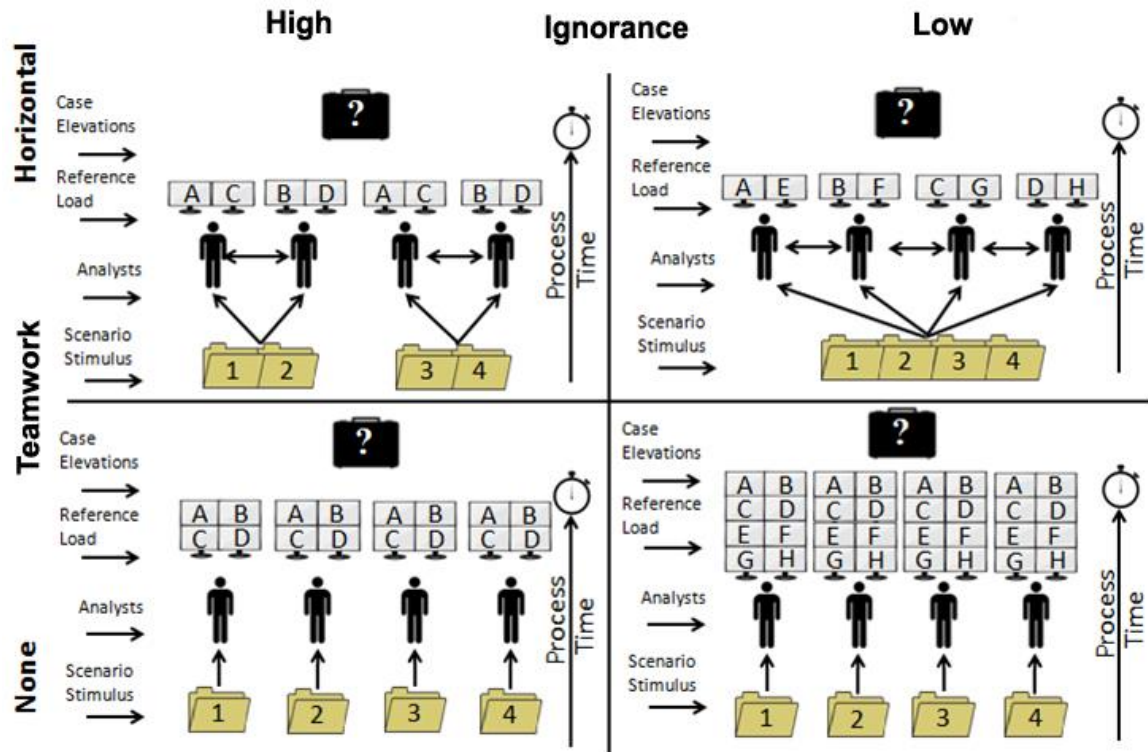
The web-based knowledge sharing environment (KSE) uses SharePoint to restrict or allow information access with role based access control (RBAC). SharePoint is a popular Microsoft product with the same look and feel of the ubiquitous Windows operating system and the Office productivity suite, featuring an intuitive interface and ease of use. SharePoint is popular among federal insider threat programs as a case management tool.

The apparatus features a networked environment directly connected to the World Wide Web under the domain “www.kellyapparatus.com.” This apparatus, accessible via personal computer (PC) running any common web browser, provides a precise means of recording elapsed time for analysis and directing individual users to specific information. It also includes a survey function to record perceptions of information overload, social impact, and ITA confidence—all relative to each participant’s preselected experimental condition.

a. How the Apparatus Functions

The apparatus contains four scenarios from the National Insider Threat Task Force (NITTF) training course that serve as the experimental stimulus. Each scenario comes with eight references—that informs both organizational and personal perspectives. The organizational perspective references inform generalizations to organizational norms. The personal perspective references are specific to the individual. An example of the organizational perspective is an email log of everyone in the organization and the personal perspective is the content of a specific person’s email. Information is presented from the general (organization) to the specific (individual), operationally defined as high and low ignorance, respectively. The SharePoint RBAC presents alternating references for each scenario, ensuring that no single participant receives the same reference twice. The experiment assigns teamwork conditions based on the ignorance assignment of participants. Teams with a high ignorance assignment consist of two people, and teams with a low ignorance assignment consist of four. Participants assigned no teamwork include those with both conditions of ignorance. Every participant in the experiment performs ITA on one scenario as independent samples. Table 7 presents the relationship between ignorance, teamwork, and scenario.

Table 7. Relationship between Ignorance, Teamwork, and Scenario.



b. Teamwork

References are individually assessed or distributed, depending on the teamwork category a participant is assigned. Participants with no teamwork access all references for one scenario. Teams assigned high ignorance receive two scenarios. Those with low ignorance assignments receive four. Each team receives specific references—then assimilates those references, and informs a single insider threat analyst of pertinent information contained within. Team participants are assigned two references each under both conditions of ignorance.

c. Ignorance

Ignorance is varied between high and low conditions. The more information the participant has, the lower the ignorance level. Non-ignorance is not testable because the participant would already know the solution to the scenario and fundamental ignorance is not testable because the participant would not know to perform ITA. This research subscribes to levels of ignorance because it deals with the lack of relevant knowledge or

information. Greater ignorance implies less information. Likewise, an analyst who is not ignorant in some respect need not perform ITA; he would simply identify the insider threat. Thus, some level of ignorance is inherent to ITA.

This research divides information into specific “references” organized by perspective. Low ignorance participants receive a total of eight references per scenario and high ignorance participants receive a total of four references per scenario. High ignorance references inform an organizational perspective of the insider, and low ignorance references inform both organizational and individual perspectives. The demarcation between perspectives uses Kelley’s (1973) covariation model to partition the references. The organization perspective allows analysts to perceive consensus behavior. The personal perspective allows analysts to perceive consistency and distinctiveness behavior. High ignorance participants are not told that they have fewer references than low ignorance participants—because the mere knowledge of missing information may change the outcome of a decision (Brem & Rips, 2000). This knowledge is controlled using the KSE’s RBAC configuration—which hides links to the additional references from high ignorance participants and ensures that no distracting “access denied” messages appear to tip them off. The KSE counterbalances references between team members, so no team member receives the same reference more than once.

d. Scenarios

Pilot testing calibrated the experiment apparatus. Pilot testers ensured there were no spelling errors and demonstrated the apparatus functioned properly.

Forty-eight additional participants comprised the experiment sample. Participants understood that all permitted information was available—and that they would only use that information to determine whether there was sufficient evidence to escalate the case to a formal investigation. No additional information was allowed, because any further inquiries could “tip off” the insider—and cause them to change their behavior and draw attention to the growing “trail of evidence.” All participants received the same instructions that incorrect responses would forfeit the performance incentive. A pre-recorded video instructed participants to role play the scenario as if they were working in

the interests of national defense—but also to be careful not to initiate unwarranted investigations that could damage someone’s career. A one-ounce silver American Eagle bullion coin provided a performance incentive that further simulated the severity of incorrect ITA. Participants understood that they would not receive the reward if their assessment was not the same as that determined by the NITTF outcome expectation.

Participants performed insider threat analysis on four similar insider threat scenarios created by the NITTF. I slightly modified the scenarios to ensure they were approximately equal in analysis time. Each participant received one of four scenarios for insider threat analysis. One scenario contained a malicious insider threat, one a non-malicious insider threat, and the remaining two contained no insider threat. I counter balanced the order of scenario presentation to account for any learning effect. The scenarios are provided in Appendix B(E).

e. Data collection

Participants evaluated each scenario on separate inter-networked PCs. The experiment proceeded through four phases: instruction, entrance survey, ITA, and exit survey. An introductory webpage oriented participants to the experiment and explained the ITA task. An instruction video demonstrated how to navigate the apparatus and perform the ITA. The introductory webpage and video were unchanged for all experiment sessions. An entrance survey collected demographic information operationalized as blocking variables. The entrance-survey items are presented in Table 8.

Table 8. Entrance Survey.

Question	Possible answers
Which most generally describes your predisposition to an accused?	Guilty until proven innocent
I am not asking how you think it should be, rather, how you are truly predisposed.	Innocent until proven guilty
Do you have any professional experience with insider threat analysis?	Threat analysis Investigations Both threat analysis and investigations No professional experience with either
How many years' experience do you have?	[Text Box]
What is your age?	[Text Box]
What is your gender?	Male Female
What is the highest level of education you have completed?	Bachelor's degree Master's degree Doctoral degree Post-Doctorate
Are you aware of the term "insider threat?"	Yes No
Server time	[Calculated value]

The participants indicated whether the case warranted escalation through a case-management survey, which was taken directly from the case worksheet provided by the NITTF insider threat course materials. References were locked and participants could not go back to assimilate more information after case creation. The apparatus locked the reference to guarantee no further ITA after the server recorded the ITA end time. The case worksheet is presented in Table 9.

Table 9. Case-Management Worksheet.

Question	Possible answers
Please describe the details of the incident (i.e., who, what, where, why, how)	Memo text box
Is this case warranted for escalation at this time?	No Yes
I feel confident that my threat assessment is correct	9-point Likert
Server time	[Calculated value]

This research sourced exit-survey items from published surveys intended to measure the perception of personal performance and information overload (Moser & Soucek, 2010; Karr-Wisniewski & Lu, 2010) and social impact (Mulvey et al., 1998). Survey items concerning perceived personal performance and information overload are presented in Table 10, while the social-impact survey items are presented in Table 11.

Table 10. Perceived Information-Overload and Personal-Performance Survey Items. Adapted from Soucek and Moser (2010).

Information Overload	Possible answers
For my scenario, I was overwhelmed by the amount of information I had to process to make a decision.	9-point Likert
Did you solve your scenario individually or with a team?	Individually Team

Table 11. Perceived Social-Impact Survey Items.
Source: Mulvey and Klein (1998).

Perceived Social Impact	Possible answers
I rushed through the task because I was considerate of my teammate's time.	9-point Likert

I evaluated each participant response for accuracy after ITA completion. Each participant who correctly answered the case according to the outcomes designated by the NITTF training course received an accuracy score of 1. Incorrect responses received a score of 0. Participants with a 1 received a Silver Eagle, as promised. The survey items, case worksheet items, and task times replicated to a master spreadsheet in real time.

4. Sample Justification

Sample size and selection were carefully considered for internal/external validity. This research considered participant eligibility to best represent the population of federal insider threat analysts and identified a convenience sampling opportunity for the best approximation to that population.

a. Participant Eligibility

The sample selection included only volunteers at the Naval Postgraduate School (NPS). The sample was selected from candidates who met the basic ITA eligibility

requirements outlined in the SPAWAR OPNAV N2N6I report, “Insider Threat Program Overview, Summary, and Recommendations.” This report was generated at the Carnegie Mellon University (CMU) CERT Insider Threat Center—a federally funded research and development center (FFRDC) that has been sponsored since 2001 by the Department of Defense (DOD) and is widely recognized as an expert authority on insider threats. The requirements outlined in the OPNAV N2N6I report restrict eligible candidates to federal employees with a top secret (TS) security clearance who are employed as GS-12 equivalents (O-3) or higher.¹¹ TS requirements imply that those cleared for TS access are cognizant of the conduct expected to hold that level clearance. The requirements for GS-12 positions imply that those eligible have at least some graduate level education.¹²

I assume that TS-cleared GS-12 and higher federal employees who are eligible for ITA positions are comparable to TS-cleared officers enrolled at NPS, because the clearance-screening requirements and educational level are similar—both are in federal service, and 96% of military students at NPS are at the O-3 pay grade or above.¹³ The TS-cleared personnel at NPS are required to maintain insider threat awareness education as a part of mandatory cybersecurity training. Thus, a good representative sample of TS-cleared NPS students and GS-12 or higher staff should generalize to similar federal employees selected for ITA positions.

b. Sample Size

The experiment leveraged a sample size of 48 divided equally between four independent test groups. Thirty is a common minimum sample size for experiments

¹¹ The general schedule (GS) classification covers the majority of civilian white-collar federal employ. Typical job requirements for insider threat analysts can be found at <https://www.usajobs.gov/GetJob/ViewDetails/448714100>; Military/general schedule equivalence chart can be found at http://comptroller.defense.gov/Portals/45/documents/fmr/archive/11aarch/11a_06_appendix_b_Dec08.pdf.

¹² Typical education requirements for DOD/Navy general schedule can be found at http://www.secnv.navy.mil/donhr/Documents/CivilianJobs/DOD_Qualification_Standard_For_GS-1102.pdf

¹³ NPS population statistics can be found at <http://nps.edu/Images/Docs/Factbook%202013%20PDF.pdf>.

published in creditable academic and industrial journals (Orcher, 2005, p. 45).¹⁴ Generally, a sample size is selected as a function of the population Z score (Z), population standard deviation (σ), and the highest acceptable deviation between the true mean and sample mean (d); e.g., $n = Z^2 \sigma^2 / d^2$ (Kerlinger & Lee, 2000, p. 297). The population standard deviation is yet unknown for this research. Drawing from Slovin's formula, when given a population size (N) and probability of error (e), "the sample size n can be obtained by the formula $n = 1 + Ne^2$ " (Guilford & Frucher, 1973, p. 13). Thus, a 48-participant randomly selected sample from a 430-person population of TS-cleared students and staff at NPS amounts to a .13 probability of error. A random sample of 208 participants would be required to reduce the probability of error to .05. For this research, several nonparametric analytic tests compensated for the low sample size. This convenience sample was necessary due to the limited number of readily available participants at NPS; however, it is acceptable because of the relatively homogenous education and training backgrounds of the participants. A convenience sample is generally acceptable for the preliminary exploration of a hypothesis (Orcher, 2005, p. 47).

5. Main Variable Operational Definitions

Teamwork is operationally defined as either horizontal specialization or none. Horizontal specialization is a classic management style that divides a functional task between specific departments. For groups containing participants assigned horizontal specialization, references are divided among individuals within a team. Participants who are assigned no specialization are presented with all references and work scenarios individually.

Ignorance is operationally defined as high or low—and measured as either four and eight references, respectively. References for this research include:

- (A) HR personnel data
- (B) SA security review

¹⁴ Sample sizes for closely related research is varies widely; i.e., n=32 (Tuttle & Burton, 1999), n=36 (Ingham et al., 1974), n=70 (Robbins, 1995), n=84 (Chidambaram & Jones, 1993), n=168 (Linden et al., 2004), n=258 (Mao et al., 2016), n=374 (Haase et al., 2014), n=457 (Stark et al., 2007), n=644 (Schippers, 2014).

- (C) CI continuous evaluation
- (D) SI supervisor interview
- (E) HR evaluations
- (F) SA access logs
- (G) CI cyber security
- (H) SI peer interview

High ignorance consists of four references (A,B,C,D), and low ignorance consists of eight (A,B,C,D,E,F,G,H). The identifying letters correspond to the references assigned to each participant, as given in Appendix B(E).

Time is operationally defined as the period in seconds that a participant uses to perform ITA.

Accuracy is operationally defined as correct or incorrect.

Confidence is operationally defined as the degree of decision confidence, using an ordinal value measured on a nine-point scale.

Perception of information overload is operationally defined as agreement with the survey statement “for my scenario, I was overwhelmed by the amount of information I had to process to make a decision,” using an ordinal value measured on a nine-point scale.

Perceived Social impact is operationally defined as agreement with the survey statement “I rushed through the task because I was considerate of my teammate’s time,” using an ordinal value measured on a nine-point scale.

6. Main Variable Attributes

Theoretical concepts are assigned meaning via operational definitions (Hughes, 1986). As a scientific theory must be falsifiable, refutable, and testable, it follows that operationally defined concepts need be measurable constructs. Proper hypotheses play a necessary role in falsifiability, because they allow scientists to subject theoretical

constructs to empirical testing.¹⁵ In this research, teamwork and ignorance are theoretical concepts that must be linked to empirical observation to validate their meaning as constructs.¹⁶ Thus, quantifiable measurement of these concepts is pursued to yield objective and empirically acceptable findings. Lord Kelvin masterfully expressed the importance of empirical observation in 1883.

I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind. (as cited in Thomson, 1889, p. 73)

The independent variables are operationalized as teamwork and ignorance. The dependent variables are operationalized as time, accuracy, performance, confidence, information overload perception, and social-impact perception.

a. Teamwork

The first nominal independent variable, teamwork, is operationally defined as horizontally specialized or none. I chose horizontal specialization because it allows analysis at the individual level. This is because only one participant makes a threat attribution at a time and the information—not the decision—is split between multiple people on a team. Analysts assigned no teamwork individually assimilate all information.

Analysts are organized based on their logon credentials to simulate either horizontal specialization or none. Each logon credential is associated with a specific scenario and reference selection. Each scenario is different, to ensure that analysts with no teamwork perform a task specific to their individual scenario. Horizontal specialization replicates the classical concept of task specificity in information processing (Daft, 2007). Separate information “departments” are each assigned specific references for shared analysis. In sum, individual participants review all references, but assess scenarios individually. Team participants review specific references individually, and then transmit the salient information to the specified analyst.

¹⁵ See Hempel 1966.

¹⁶ See Feigl, 1970.

Teamwork participants may not view the references on another participant's screen, transfer screen shots, or email copied-and-pasted operations to bypass the RBAC. All team members are allowed to view the same scenario stimuli, but only the designated participant may perform ITA for his assigned scenario. The designated participant for the particular scenario must retrieve information from his team mates to complete ITA. For each scenario, one participant plays the role of insider threat analyst—and only that role has access to all available information. The remaining members serve as support staff who assimilate information contained in multiple references and transmit pertinent information to the insider threat analyst. As in a relay race, each participant passes the baton to the next participant for ITA of a subsequent scenario. ITA is complete when the team has performed ITA on one scenario per participant. Table 12 presents the experimental relationships between scenario, teamwork, and ignorance.

Table 12. Participant Scenario and Reference Assignments.

Participant	Scenario	Scenario 1 Refs	Scenario 2 Refs	Scenario 3 Refs	Scenario 4 Refs	Scenario1
G1SHRLP1	1 2	A C	B D			RefA = HR Personnel
G1SHRLP2	1 2	B D	A C			RefB = Security Review
G1SHRLP3	3 4			A C	B D	RefC = Continuous Eval
G1SHRLP4	3 4			B D	A C	RefD = Peer Interview
G1SHRHP1	1 2 3 4	A E	B F	C G	D H	RefE = Supervisor Interview
G1SHRHP2	1 2 3 4	B F	C G	D H	A E	RefF = CyberSecurity
G1SHRHP3	1 2 3 4	C G	D H	A E	B F	RefG = Access Logs
G1SHRHP4	1 2 3 4	D H	A E	B F	C G	RefH = HR Evaluation
G1SLRLP1	1	A B C D	A B C D	A B C D	A B C D	
G1SLRLP2	2	A B C D	A B C D	A B C D	A B C D	
G1SLRLP3	3	A B C D	A B C D	A B C D	A B C D	
G1SLRLP4	4	A B C D	A B C D	A B C D	A B C D	
G1SLRHP1	1	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	
G1SLRHP2	2	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	
G1SLRHP3	3	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	
G1SLRHP4	4	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	
G2SHRLP1	1 2	A C	B D			
G2SHRLP2	1 2	B D	A C			
G2SHRLP3	3 4			A C	B D	
G2SHRLP4	3 4			B D	A C	
G2SHRHP1	1 2 3 4	A E	B F	C G	D H	
G2SHRHP2	1 2 3 4	B F	C G	D H	A E	
G2SHRHP3	1 2 3 4	C G	D H	A E	B F	
G2SHRHP4	1 2 3 4	D H	A E	B F	C G	
G2SLRLP1	1	A B C D	A B C D	A B C D	A B C D	
G2SLRLP2	2	A B C D	A B C D	A B C D	A B C D	
G2SLRLP3	3	A B C D	A B C D	A B C D	A B C D	
G2SLRLP4	4	A B C D	A B C D	A B C D	A B C D	
G2SLRHP1	1	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	
G2SLRHP2	2	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	
G2SLRHP3	3	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	
G2SLRHP4	4	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	
G3SHRLP1	1 2	A C	B D			
G3SHRLP2	1 2	B D	A C			
G3SHRLP3	3 4			A C	B D	
G3SHRLP4	3 4			B D	A C	
G3SHRHP1	1 2 3 4	A E	B F	C G	D H	
G3SHRHP2	1 2 3 4	B F	C G	D H	A E	
G3SHRHP3	1 2 3 4	C G	D H	A E	B F	
G3SHRHP4	1 2 3 4	D H	A E	B F	C G	
G3SLRLP1	1	A B C D	A B C D	A B C D	A B C D	
G3SLRLP2	2	A B C D	A B C D	A B C D	A B C D	
G3SLRLP3	3	A B C D	A B C D	A B C D	A B C D	
G3SLRLP4	4	A B C D	A B C D	A B C D	A B C D	
G3SLRHP1	1	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	
G3SLRHP2	2	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	
G3SLRHP3	3	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	
G3SLRHP4	4	A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H	

b. Ignorance

The second categorical independent variable, ignorance, is operationally defined as high or low. Kelley's Covariation Model informed the reference partition per organizational or personal perspectives. Participants assigned high ignorance are given references that primarily inform an organizational perspective requiring greater reliance on recognition to "fill in the gaps." Participants assigned low ignorance are given references that inform both organizational and individual perspectives. For instance, a security review differs from access logs in perspective. The security review contains general information about deviations from organizational norms, whereas access logs contain information specific to the individual. As a result, the security review primarily informs an organizational perspective and access logs primarily inform a personal perspective. High ignorance groups receive references that inform the organizational perspective because "consensus," an organizational perspective term, is the first consideration in Kelley's covariation model. Low ignorance groups receive references that inform both organizational and personal perspectives. The organizational perspective informs the consensus component of Kelley's covariation model and the personal perspective informs the consistency and distinctiveness components.

(1) High Ignorance

High ignorance presents the participant with four references that were generated by Agency XYZ (a fictitious organization): personnel data, security review, continuous evaluation, and peer interview.

- The personnel file (A) contains employee information—including the insider's marital status, family members, contact information, salary, job title, clearance level, work history, and disciplinary actions—to inform the perception of organizational fit of the insider under review.
- The security-review file (B) contains compartment-access records, a summary of physical access, and a summary of computer access. The security-review file provides a technical perspective on the level of access the insider holds within the agency.
- The continuous-evaluation file (C) contains external database information—including financial history, criminal history, and passport records—to reveal the consensus aspect on the insider's activities.

- The peer interview (D) is an assessment of the insider from the perspective of a fellow employee. The peer interview provides the analyst with an organizational perspective.

(2) Low Ignorance

The low ignorance condition presents participants with all of the references provided under the high ignorance condition, along with an additional four that include more specific personal details and history.

- The insider-evaluation report (E) details individual work performance and duties. The insider-evaluation report offers evidence to determine the consistency of the insider's performance.
- Detailed access logs (F) reveals individual physical accesses. The access logs reveal the consistency of access patterns.
- The cybersecurity report (G) details individual user activity monitoring and data flows to and from foreign network domains. The cybersecurity report provides information that allows the analyst to evaluate if information flows are anomalous among co-workers.
- The supervisor interview (H) provides a specific assessment of the insider from the perspective of the insider's supervisor. The supervisor interview reveals the distinctiveness of the insider's behavior.

The relationship between references and individuals is illustrated in Table 12. These references are selected as consistent with guidance from CNSS directive 504, NITTF-2014-008, and a number of scholarly publications (Guido & Brooks, 2013; Maybury et al., 2005; Brackney & Anderson, 2004). All references and scenario stimuli are found in Appendix B.

c. ITA Time

The clock starts when analysis begins and stops when the participant commits to creating a case by initiating a case-management survey. I operationalize analysis starting time as the submission time of the entrance survey, because each participant is immediately presented a case stimulus after he completes the survey. I operationalize analysis ending time as the moment a participant commits to creating a case, because the actual recording of case details is ancillary to threat analysis. Analysis starting and ending times are automatically recorded by the KSE software.

The starting time for analysis by non-specialized participants is straightforward, but the starting time for team analysis must accommodate the interrelationships of the ITA team. Team analysis starting time is operationalized as the moment the last team member completes the entrance survey, because all team members must perform analysis simultaneously on each scenario. I assigned each participant to a specific scenario at the beginning of the experiment and counter balanced the scenario order between teams. Team members progress from one scenario to the next with a single participant responsible for an assigned scenario. The time each prior case is submitted is also the start time of the following ITA.

d. ITA Accuracy

The second component of performance in the experiment is accuracy, specifically whether a participant correctly identifies the insider threat. Scenario outcomes are assessed according to the NITTF-recommended outcomes in Appendix B(C)(2). I operationalize accuracy as a dichotomous value—assigning each correct ITA a score of 1, and each incorrect ITA a score of 0.

Correct responses to scenario stimuli require participants to identify risk factors from the “adjudicative guidelines for determining eligibility for access to classified information” (2016; Carney and Marshall-Mies, 2000). Participants received as much time as they required to review the adjudicative guidelines prior to the start of the experiment. To simply state that behavior looks suspicious is insufficient. Participants investigate given references and explain why they perceive that an insider is a threat. That is to say, each participating analyst will use knowledge from the required TS clearance insider threat training and the adjudicative guidelines to discern insider threats.

ITA performance measure is highly dependent on accuracy, though the accuracy measure is binary. A ceiling effect from correct analysis would make ITA time and ITA performance basically the same measure. Additional dependent measures—including ITA decision confidence, social-impact perception, and information-overload perception—increase the explanatory power of the experiment results in the case of overwhelming correct answers in all test groups.

e. ITA Performance

Performance is basically a measure of effectiveness (Maizlish & Handler, 2005, p. 53), which is generally the capacity to produce a desired outcome in a work process. common desired outcome is to produce as much as possible using minimal time and resources. This implies, *ceteris paribus*, that an insider threat analyst who quickly identifies a threat performs better than one who spends greater time on the same identification. It follows inversely that an insider threat analyst who fails to identify an insider threat—but wastes little time in the process—performs better than one who wastes more time on the same failure.

According to NITTF, insider threat programs within the federal government generally benchmark against each other (see NITTF communication in Appendix A). I operationalize performance as an objective measure, calculated by benchmarking insider threat analyst performances against each other. In this way, I assess individual performance using the same method as current insider threat programs.

Following Jaquith (2007, p. 25), performance metrics must be both simple and expressed as a percentage. I transform the ITA performance value to account for both correct and incorrect responses along a scale from 0 to 2. An insider threat analyst who takes longer to reach an incorrect answer receives a lower score than one who spends less time on an incorrect answer. No incorrect answers may result in a score of 1 or greater, and no correct answer may result in a score less than 1. I transformed analysis time to a scale of 0–1 to make the time values more meaningful for comparison between groups and individuals. Equation 1 illustrates the ITA time transformation.

$$ITATimeScore = \frac{GreatestAnaysisElapsedTime - SpecificElapsedTime}{GreatestAnalysisElapsedTime}$$

Equation 1. ITATimeScore

ITA Performance is operationally defined as ITA Time plus accuracy score. I transformed the performance score to make it more meaningful for comparison. The transformed performance score follows the form in Equation 2.

$$Performance = ITATimeScore + ITAAccuracy$$

Equation 2. Performance Transform

I give the performance value greater meaning at the individual level by accounting for both incorrect and correct answers. The ITA Performance measure is calculated on a scale from 0 to 2 to simultaneously identify time and accuracy. Performance is transformed to a percentage in Figure 2 and 3 to comply with Jaquith's (2007, p. 25) concept of performance that is expressed in time and as a percentage.

Since analysts must process a continuous stream of threat indicators, I consider the effects of time spent in incorrect analysis. Insider threats are known to leave a trail of evidence that consists of many indicators (Cappelli et al., 2012). I infer that the more time taken to arrive at an incorrect conclusion, the less time available for further threat analysis. I code both analysis time and accuracy values in such a way that both correct and incorrect ITA performance scores are meaningful.

f. ITA Confidence

ITA decision confidence is necessary because accuracy is a binary variable. Given the small sample size used for this experiment, random guesses may create a perception of higher performance—whereas in reality, the relationship between these factors may be nothing more than chance. Higher confidence implies that an accurate ITA decision is less likely the result of chance. I employ a nine-point Likert-type scale because previous research implies that an 11-point scale may be too complex and a five-point scale lacks sufficient resolution (Mead and Moseley, 2001). Scheibe, Skitsch, and Schofer (1975) find that participants most easily understand nine-point Likert items. Furthermore, Likert items have interval-level properties when they have descriptive adjectives (Von der Gracht, 2008). The Likert items in this experiment are derived from past-validated research surveys, with the exception of one ITA confidence item.

g. Information-Overload Perception

Information-overload perception measures the effects of ignorance and teamwork as factors of information overload when time is not a factor in decision making. For this experiment, participants complete a pre-validated survey to measure their perception of information overload (Moser & Soucek, 2010; Karr-Wisniewski & Lu, 2010). The effects of information overload may explain variance in ITA accuracy and time. The information-overload perception value is the average of survey-item scores.

h. Social-Impact Perception

Social-impact perception measures the effect that ignorance has on the social information exchange between participants. This measure reveals whether ignorance variations or teammates' loafing best explains variability in analysis time and accuracy. This experiment measures social impact with a pre-validated survey (Mulvey et al., 1998). The social-impact perception value is the average of survey-item scores.

7. Blocking Variable (Demographics) Operational Definitions

Blocking variables are operationally defined as follows:

- *Experience* is professional familiarity with ITA-relevant effect relationships that informs intuition; an interval value, each interval is measured as one year's worth.
- *Age* is time alive; an interval value, each interval is measured as one year.
- *Education* is highest degree obtained; an ordinal value with four categories: bachelor's degree, master's degree, doctoral degree, and post-doctoral degree.
- *Gender* is chromosomal sex category; a binary categorical value: male or female.

8. Blocking Variable (Demographics) Attributes

The main research variables—teamwork and ignorance—may have effects explained by the sample selection. Research design does not account for the effects that experience, age, education, experience type and gender may have on the dependent variables. This research uses blocking variables to control for variability caused by

factors not specifically identified in the main research design. Blocking variables are the properties of the individual participant—including experience, experience type, age, education, and gender. These variables arrange participants into groups (viz., blocks) that are similar—and as a result, they become variables that may account for some of the variation in dependent variable that is explained by demographics.

a. Experience

Experience is an ordinal value measured in number of years. Expertise tends to develop in a predictable manner (Dreyfus, 2004). Dreyfus does not offer a time bracket such as Herbert Simon's (1996) ten-years-to-expert, or Malcolm Gladwell's (2008) 10,000-hour rule. However, the Dreyfus model of skill acquisition describes a five-stage progression from novice to expert that is sequential and additive. According to Dreyfus, novices learn to follow rules; advanced beginners memorize the rules; competents know why the rules apply, and where; proficients intuitively recognize the situations in which rules apply; and experts intuitively know the effects of their decisions. Thus, experience could explain some variability in the dependent variables.

b. Age

Age is transformed to an ordinal value that measures maturity,¹⁷ as age is a better indicator of maturity than expertise. Though an older person is not always mature, age is generally regarded as a rule-of-thumb correlative. Some participants, especially female, may take a hiatus from their profession to rear children, and economic downturns may have interrupted gainful employment for both sexes. Participants of an older age are likely to have additional life experiences that inform ITA.

c. Gender

Gender is a binary categorical variable determined by sex at birth. Brain function, structure, and chemistry are known to differ with gender (Cosgrove, Mazure, and Staley, 2007), which can cause variability during ITA—e.g., in suspicion or apathy. Blocking by

¹⁷ Merriam-Webster defines maturity as a quality of “full development.”

gender, this study controls for the effects of gender on ITA performance, perceptions of information overload, and ITA decision confidence.

d. Education

Education accounts for the variance caused by the academic maturity of participants. Education is known to have a relationship with intelligence and there are various interpretations of that relationship (Ritchie, Bates and Deary, 2015). I assess education as the highest academic degree completed rather than years in academia, because more time in school does not necessarily mean more education—e.g., five versus three years for a bachelor’s degree could be due to a military deployment or financial factors. The product is the same degree, regardless of time that is otherwise measured by age or experience.

B. JUSTIFICATION FOR LABORATORY EXPERIMENTATION

The circumstances of the research are used to determine whether qualitative or quantitative methods are used in a given inquiry (Glaser & Strass, 1967, p. 18). Qualitative methods are generally used to generate a theory or probe a topic to get a sense of the theory base (Creswell, 2014, p. 110). The theory that emerges may then be verified with a quantitative method, such as laboratory experimentation (Jarvenpaa, 1988). As a qualitative foundation for this research, I probed the state of ITA with site visits, game mastered a massive multiplayer online war-game leveraging the Internet (MMOWGLI) (Mascolo, 2016), and made a qualitative data assessment of insider threat experts (outlined in Appendix D) cited in Kelly and Anderson (2016). The next step is theory testing per the “advancement of knowledge” continuum illustrated in Jarvenpaa (1988) and mentioned in Newman and Benz (1998, p. 13).

Laboratory experimentation is advantageously employed when the research question begins with “how,” the researcher has control over variables, and the research is not focused on historical events (Yin, 2014, p. 9). The laboratory is an environment in which the researcher may control for confounding variables to produce replicable knowledge (Kerlinger & Lee, 2001). To these observations, I add that knowledge generated

through laboratory experimentation is more easily defended than other forms of knowledge.

Pursuant to SECNAVINST 3900.39, NPS requires Institutional Review Board (IRB) approval for human-subjects research, as employed in this research. DODI 3216.02 prohibits monetary compensation to federal employees as a method of participant coercion. This research provides monetary compensation in the research design, but not as a recruitment contrivance. Approval was obtained for this experiment, as provided in Appendix C.

C. SUMMARY

This chapter presented the research in a 2 x 2 factorial design. The design includes two main predictor variables, ignorance and teamwork, that this chapter described and operationally defined. The chapter also described and defined design blocking variables including age, gender, education, experience, and experience type. The design presented five dependent variables—ITA time, accuracy, confidence, perception of information overload, perception of social impact—and a dependent performance measure, ITA performance, calculated from ITA time and accuracy.

This section described the sample selection requirements, sample size, and presented evidence that the sample is suitable for this research. The participants, who constitute a convenience sample, closely resembles the population of insider threat analysts according to security clearance, education, and pay grade.

This chapter outlines a laboratory experiment apparatus capable of collecting data for testing the effects of teamwork and ignorance on ITA performance. The role based access control capabilities of a KSE, SharePoint, are leveraged to manipulate the independent variables. An experimental environment is established using an online data-collection device (<http://www.kellyapparatus.com>). The KSE maintains survey responses and analysis time for each individual participant and organizes the results in an Excel spreadsheet. Performance measures are assessed as time and accuracy at the individual level of analysis, in a highly controlled and repeatable manner. The scripts necessary to

precisely recreate the web-based apparatus, along with the insider threat scenarios and references, are provided in Appendix B.

Chapter III examines the characteristics of the data collected by the experiment apparatus and the statistical methods for analysis. I reduced the main research question (“how do ignorance and teamwork affect analyst accuracy, time, and confidence?”) to 50 ancillary research questions. Each ancillary question supports the research with specific analytical method selection based on the characteristics of the data. Chapter IV presents the results of the data analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DATA ANALYSIS

Chapter II explored the academic literature relative to the main research question “how does ignorance and teamwork affect analyst time and accuracy?” Chapter III outlines how the specific data are collected with the experimental apparatus for hypothesis testing. This research included several ancillary research questions to investigate each hypothesis. I include several blocking variables within the data analysis to better define the theoretical relationships between independent and dependent variables. The blocking variables were not included in the main research question, but preceded from ancillary questions. Each ancillary question compels a specific analysis method suitable to the data type.

This chapter describes the analytical framework of the research design, including main and supporting inquiries. This work first statistically addresses the primary research questions with ancillary questions via several descriptive statistical methods. Descriptions of data characteristics justify the selection of the non-parametric tests covered in Chapter V. This chapter closes with assessments of internal and external validity.

A. ANALYTICAL FRAMEWORK

This research demonstrates a two-part analysis to answer ten primary research questions. The research questions compel specific analytical methods to evaluate the causal effects of the predictor variables based on variable level. This work addresses each primary research question with several specific ancillary research questions.

1. Primary Research Questions

This research tests theories of attribution and process loss with ten primary research questions. 50 ancillary research questions were derived from the ten primary research questions and two supporting research questions. The primary research questions were:

- Does ignorance affect ITA accuracy?
- Does ignorance affect ITA time?

- Does ignorance affect ITA confidence?
- Does teamwork affect ITA accuracy?
- Does teamwork affect ITA time?
- Does teamwork affect ITA confidence?
- Does ignorance affect perceptions of information overload?
- Does teamwork affect perceptions of information overload?
- Does ignorance affect perceptions of social impact?
- Do teamwork and ignorance interact?

The supporting research questions were:

- Do demographics affect ITA time, accuracy, confidence, social impact, and information overload?
- Are there any statistically significant differences between experiment stimuli that could cause an experimentally fixed effect?

2. Analytical Methods

This research leverages a web server to submit questionnaires to each participant and record the elapsed time of analysis. Accuracy is the only categorical dependent variable and compels a binary logistical-regression-analysis method. ITA time is a continuous variable measured in seconds. Together, the two measures (accuracy and time) are a coded performance ratio on a continuum between 0–2.

I assign teamwork and ignorance as dichotomous categorical variables identified by a participant's web server logon credentials. Each of the four categorical conditions of specialization and ignorance are represented by 12 participants, for a total of 48 participants. Table 13 presents independent and dependent variable data types.

Table 13. Independent and Dependent Variables.

Independent variables (Data): Teamwork (0/1) Ignorance (0/1) Age (# Years) Gender (0/1) Education (1–4) Experience (# Years) Scenario (1,2,3,4) Outcome (0/1)	Dependent variables (Data): Insider threat analyst time (# seconds) Insider threat analyst Accuracy (1/0) Insider threat analyst performance (ratio) Insider threat analyst decision confidence (1–9) Information overload perception (1–9) Social impact perception (1–9)
--	---

Variable data types are in parentheses.

Table 14 lists specific questions derived from the more general research questions. Statistical tests are specific to certain data types; while statistical analysis methods may allow a combination of questions in a single analytical method, some questions require divisions among analytical methods because of variations in data types. For instance, accuracy, a dependent categorical variable, compels either a chi-square test or a logit regression, depending on the nature of the independent variable. This work leverages non-parametric tests to bolster the results of the parametric tests. Table 14 summarizes 50 supporting research questions, data types, and statistical analysis methods.

Table 14. Ancillary Research Questions, Variables, and Statistical Analysis Method.

Main Research Questions		[Independent (data)] <Dependent(data)>	Analysis
1	Does teamwork and ignorance interactively affect analyst performance?	INDEP: Team(0/1); Ign (0/1) DEP: performance(ratio)	ANOVA
2	Does teamwork affect analyst performance?	INDEP: Team(0/1) DEP: performance(ratio)	ANOVA Regression Mann Whitney U
3	Does ignorance affect analyst performance?	INDEP: Ign(0/1) DEP: performance (ratio)	ANOVA Mann Whitney U Regression
4	Does teamwork and ignorance interactively affect analyst time?	INDEP: Team(0/1); Ign(0/1) DEP: Time (# seconds)	ANOVA
5	Does teamwork affect analyst time?	INDEP: Team(0/1) DEP: Time (# seconds)	ANOVA Regression Mann Whitney U
6	Does ignorance affect analyst time?	INDEP: Ign(0/1) DEP: Time (# seconds)	ANOVA Regression Mann Whitney U
7	Does teamwork and ignorance interactively affect analyst accuracy?	INDEP: Team(0/1); Ign(0/1) DEP: Accuracy (0/1)	ANOVA
8	Does teamwork affect analyst accuracy?	INDEP: Team(0/1)	Logit Regression

Main Research Questions		[Independent (data)] <Dependent(data)>	Analysis
		DEP: Accuracy(0/1)	Chi-square test
9	Does ignorance affect analyst accuracy?	INDEP: Ign(0/1) DEP: Accuracy(0/1)	Logit Regression Chi-square test
10	Does teamwork and ignorance interact with analyst confidence?	INDEP: Team(0/1); Ign(0/1) DEP: Confidence(1–9)	ANOVA
11	Does teamwork affect analyst confidence?	INDEP: Team(0/1) DEP: Confidence(1–9)	Regression Mann Whitney U
12	Does ignorance affect analyst confidence?	INDEP: Ign(0/1) DEP: Confidence(1–9)	Regression Mann Whitney U
13	Does teamwork and ignorance interactively affect perceptions of information overload?	INDEP: Team(0/1); Ign(0/1) DEP: InfoOvld(1-9)	ANOVA
14	Does teamwork affect perceptions of information overload?	INDEP: Team(0/1) DEP: InfoOvld(1-9)	Regression Mann Whitney U
15	Does ignorance affect perceptions of information overload?	INDEP: Ign(0/1) DEP: InfoOvld(1-9)	Regression Mann Whitney U
16	Does ignorance affect perceptions of social impact?	INDEP: Ign(0/1) DEP: InfoOvld(1-9)	ANOVA Mann Whitney U

Fixed effects questions:		[Independent (data)] <Dependent(data)>	Analysis
17	Does any scenario affect analyst time?	INDEP: Scenario(1–4) DEP: Time (# seconds)	ANOVA Regression Kruskal-Wallis
18	Does scenario outcome affect analyst time?	INDEP: Outcome(0/1) DEP: Time (# seconds)	ANOVA Regression Mann Whitney U
19	Does any scenario affect analyst performance?	INDEP: Scenario(1–4) DEP: performance(ratio)	ANOVA Regression Kruskal-Wallis
20	Does scenario outcome affect analyst performance?	INDEP: Outcome(0/1) DEP: performance(ratio)	ANOVA Regression Mann Whitney U
21	Does any scenario affect analyst accuracy?	INDEP: Scenario(1–4) DEP: accuracy(0/1)	Logit Regression Chi-square test
22	Does scenario outcome affect analyst accuracy?	INDEP: Outcome(0/1) DEP: accuracy(0/1)>	Logit Regression Chi-square test
23	Does any scenario affect analyst decision confidence?	INDEP: Scenario(1–4) DEP: confidence(1–9)	ANOVA Regression Kruskal-Wallis

24	Does scenario outcome affect analyst decision confidence?	INDEP: Outcome(0/1) DEP: confidence(1-9)	ANOVA Regression Mann Whitney U
25	Does any scenario affect perceptions of information overload?	INDEP: Scenario(1-4) DEP: InfoOvld(1-9)	ANOVA Regression Kruskal-Wallis
26	Does scenario outcome affect perceptions of information overload?	INDEP: Outcome(0/1) DEP: InfoOvld (1-9)	ANOVA Regression Mann Whitney U
Blocking variable questions:		[Independent (data)] <Dependent(data)>	Analysis
27	Does age affect analyst time?	INDEP: Age(#years) DEP: Time(# seconds)	Regression
28	Does gender affect analyst time?	INDEP: Gender(0/1) DEP: Time(# seconds)	Regression
29	Does education affect analyst time?	INDEP: Education(1-4) DEP: Time(# seconds)	Regression
30	Does experience affect analyst time?	INDEP: Experience(#years) DEP: Time(# seconds)	Regression
31	Does age affect analyst accuracy?	INDEP: Age(#years) DEP: Accuracy(0/1)	Logistic regression

32	Does gender affect analyst accuracy?	INDEP: Gender(0/1) DEP: Accuracy(0/1)	Logistic regression
33	Does education affect analyst accuracy?	INDEP: Education(1–4) DEP: Accuracy(0/1)	Logistic regression
34	Does experience affect analyst accuracy?	INDEP: Experience(#years) DEP: Accuracy(0/1)	Logistic regression
35	Does age affect analyst performance?	INDEP: Age(#years) DEP: Performance(ratio)	Regression
36	Does gender affect analyst performance?	INDEP: Gender(0/1) DEP: Performance(ratio)	Regression
37	Does education affect analyst performance?	INDEP: Education(1–4) DEP: Performance(ratio)	Regression
38	Does experience affect analyst performance?	INDEP: Experience(#years) DEP: Performance(ratio)	Regression
39	Does age affect analyst confidence?	INDEP: Age(# years) DEP: Confidence(1–9)	Regression
40	Does gender affect analyst confidence?	INDEP: Gender(0/1) DEP: Confidence(1–9)	Regression
41	Does education affect analyst confidence?	INDEP: Education(1–4) DEP: Confidence(1–9)	Regression

42	Does experience affect analyst confidence?	INDEP: Experience(#years) DEP: Confidence(1-9)	Regression
43	Does age affect the perception of information overload?	INDEP: Age(#years) DEP: InfoOvld(1-9)	Regression
44	Does gender affect the perception of information overload?	INDEP: Gender(0/1) DEP: InfoOvld(1-9)	Regression
45	Does education affect the perception of information overload?	INDEP: Education(1-4) DEP: InfoOvld(1-9)	Regression
46	Does experience affect the perception of information overload?	INDEP: Experience(#years) DEP: InfoOvld(1-9)	Regression
47	Does age affect the perception of social impact?	INDEP: Age(#years) DEP: SocImpact(1-9)	Regression
48	Does gender affect the perception of social impact?	INDEP: Gender(0/1) DEP: SocImpact(1-9)	Regression
49	Does education affect the perception of social impact?	INDEP: Education(1-4) DEP: SocImpact(1-9)	Regression
50	Does experience affect the perception of social impact?	INDEP: Experience(#years) DEP: SocImpact(1-9)	Regression

B. DEPENDENT VARIABLE STATISTICAL CHARACTERISTICS

The characteristics of the dependent variable determined the appropriate statistical methods for each. Dependent variable data—including the accuracy, time, performance, and confidence of individual insider threat analyses—offer evidence that predicts the performance effects of teamwork and ignorance. This section describes the findings from descriptive statistics.

The insider threat experiment divided 48 participants into four test groups of 12 each. One group was evaluated under conditions of horizontally specialized teamwork and low ignorance, one under conditions of no teamwork and low ignorance, one under conditions of horizontally specialized teamwork and high ignorance, and the remaining under conditions of no teamwork and high ignorance.

1. Descriptive Statistics

This section outlines some descriptive statistics for performance, time, accuracy, confidence, information overload, and social impact data. The descriptive statistics show that analysis time ranged from 390 seconds for the fastest assessment to 2022 seconds for the slowest assessment. The average time to perform ITA was about 15 minutes. Participants were about 40% more accurate than not and were generally confident in their assessments and the accuracy score was reflected in the performance score. Information overload and social impact perceptions were generally low under all experimental conditions. Table 15 presents descriptive statistics from 48 participants in four test groups for range, mean, standard deviation and variance.

Table 15. Descriptive Statistics—Range, Mean, Standard Deviation, and Variance.

	N	Range	Mean	Std. Deviation	Variance
Performance	48	1.5093	1.2515	.4582	.210
Time	48	1632	923.71	384.122	147549.615
Accuracy	48	1	.71	.459	.211
Confidence	48	4	7.17	1.191	1.418
InfoOvld	48	4	1.94	1.174	1.379
SocImpact	24	3	1.83	1.049	1.101

Data skewness reveals the asymmetry of the distribution (Field, 2013, p. 20). Time data was negatively skewed, indicating that there are some outliers who took an extraordinary time to complete the assessment. The negative skew in performance and accuracy scores together indicate that participants assessed scenarios correctly more so than incorrectly, and did so within relatively similar times. The high positive information overload and social impact skew indicates that the participants were seldom overloaded and overall, perceived little social impact. Tests of normality and visual representations of the distributions are covered in (Appendix E).

Kurtosis tests reveal the height of the distribution central peak relative to the tails. The negative kurtosis of Performance data is due to the bimodal distribution created by the performance transform. The negative kurtosis in confidence data indicates that confidence scores were relatively even across the scale. The negative Accuracy kurtosis indicates that participants assessed scenarios accurately more than not. Table 16 presents descriptive statistics that describe the skewness and kurtosis of the data distributions.

Table 16. Descriptive Statistics—Skewness and Kurtosis.

	N	Skewness		Kurtosis	
	Statistic	Statistic	Std. Error	Statistic	Std. Error
Performance	48	-.675	.343	-1.014	.674
Time	48	.950	.343	.841	.674
Accuracy	48	-.947	.343	-1.154	.674
Confidence	48	.137	.343	-.872	.674
InfoOvld	48	1.277	.343	.953	.674
SocImpact	24	1.099	.472	.084	.918

2. Correlation

The dependent variables ITA time, accuracy, confidence, and perception of information overload are not highly correlated. High correlation implies that the dependent variables are measuring the same thing. High correlation is greater than .8 (Field, 2013, p. 686). ITA performance and accuracy are highly correlated, because performance is measured as accuracy within a percentage of the highest analysis time. Although ITA performance is highly correlated with accuracy, it introduces an added benefit of measuring incorrect analysis against other incorrect analysis. Table 17 presents a matrix that presents correlations between the dependent variables.

Table 17. Correlation Matrix—Time, Accuracy, Performance, Confidence, Information Overload.

	Time	Accuracy	Performance	Confidence	InfoOvld
Time	1				
Accuracy	0.212($p=.147$)	1			
Performance	-0.201($p=.169$)	0.914($p=.000$)	1		
Confidence	0.075($p=.611$)	0.285($p=.049$)	0.254($p=.081$)	1	
InfoOvld	0.075($p=.610$)	0.044($p=.765$)	0.013($p=.929$)	-0.129($p=.381$)	1

C. VALIDITY

Validity informs us whether the inferences to be drawn are meaningful and useful when applying scores from particular instruments (Yin, 2014, p. 46). Validity is categorized as internal and external. Internal validity assumes an objective epistemology; thus, the evidence appears valid depending on the statistical significance of the results. Internal validation concepts, beyond face validity, are generally measures of reliability. External validity is a claim of generalizability to something other than a specific experiment. It asks “how much does the experiment agree with the real world?” Both the internal and external validity of experimental results are assessed in this investigation.

1. Threats to Internal Validity

Causal relationships are validated scientifically by considering relationships in terms of statistical probability. There are threats to the validity of the inferences made from measurements when a researcher is not measuring what he intends to measure due to illusory correlations. Of the 11 documented threats to internal validity (Creswell, 2014; Graziano & Raulin, 1993; Campbell & Stanley, 1963), six are particularly relevant to this study.

History is the greatest threat to internal validity. While the historical effect in this experiment is small for individual participants presented with just one scenario, an historical effect may manifest for those assigned to four-person teams who participate in four scenarios. They may tire of performing ITA, and perform worse with each new scenario—or conversely, they may warm up and perform better. They may adhere to imaginary time constraints and work to that anxiety instead of performing diligent ITA. I mitigated this threat to internal validity by asking all participants to perform ITA without intermission, in order to maintain focus. In addition, I issued one scenario per participant and informed them that they would receive compensation based solely upon the proper analysis of that scenario alone. The effects of social loafing were controlled by introducing individual accountability and compensation. I explained to participants that time is not a factor in their compensation, but request that they work as fast as possible to

accomplish ITA. Furthermore, participants were not informed about successful ITAs until after the exit survey was complete.

Maturation is a threat to internal validity because participants will improve at scenario assessment as they progress. Because each scenario is different, participants get better at assessing them by learning what to look for in the references and neglecting non-pertinent information. I controlled for the effects of maturation by randomizing the order in which references were presented. No participant received the same reference twice, and therefore, they could not simply prune unnecessary information within the reference a priori. Access control features in the KSE prevented anyone but the intended recipient from viewing any reference under any scenario. The relationships among participant, scenario, and reference are given in Appendix B(B)(3).

A sample selection that includes a participant who is knowledgeable about ITA may severely bias the results, because the presence of a team expert should elevate the relative expertise of the entire subgroup (Benner, 2009). To control for this threat, participants were screened for previous experience with the NITTF scenarios used in the experiment.

No mid-experiment tweaks to instrumentation were made, as they might have biased the results of the experiment. Problems or missing information that came to light during the experiment applied to all participants. The experiment excluded information by design—otherwise, it would be a well circumscribed problem-solving exercise that relies heavily on deductive reasoning.

There was no compensatory rivalry among groups; the groups did not know which received treatment. Each participant evaluated one scenario and is rewarded equally for a correct ITA. Individuals were not told they would be compared with other configurations of ignorance and teamwork. The KSE concealed the presence of additional scenarios and references with RBAC.

Temporal separation among subgroups reduced the possibility of communication among them and mitigated the diffusion of treatment effects. Nevertheless, it is possible that some participants may inform others of the correct responses to their assigned ITA

scenario, in defiance of a nondisclosure agreement. Participants were unable to observe others while awaiting their turn, and participants did not know who would perform subsequent insider threat analysis. The participants also knew that they observed one of several potential scenarios, so they would expect their ITA to differ from that of another participant.

2. Threats to External Validity

This experiment tested theories of attribution and process loss using ITA as a test case to make inferences about latent theoretical concepts; thus, the experiment is susceptible to three threats to external validity.

The participant selection may interact with research bias to threaten the external validity of the results. According to former-president George W. Bush, “the best and brightest military officers from the United States and around the world come to the Naval Postgraduate School.” The cognitive capacity of NPS students is generally high and may not generalize to the broad insider threat analyst population. Furthermore, the teamwork skills that NPS students learn in military service may cause the teamwork condition to have a different effect on ITA performance than it would for teams comprised of insider threat analysts who do not have military training.

The setting of an experiment interacting with the results may also threaten external validity. Laboratory tests in the social sciences have a novelty effect, and the online apparatus may not properly capture how insider threat analysts perform their duties (Mayo, 1933). The experiment controls for the interaction of setting by using training scenarios written specifically for use in a similar setting. The scenarios were presented in an online format that is the same across all groups.

Recent high-profile insider threat attacks have increased awareness of risk within the military and general population, and the interaction of historical events on the experiment may pose a threat to external validity. To reduce the effects of historical interaction, the scenarios presented are obscure and non-sensational.

D. SUMMARY

This chapter distilled the main research question into eight primary research questions. The primary research questions quantify the relationship between each independent and dependent variable. This chapter reduced the primary research questions into 50 ancillary and supporting research questions that examine the effects of blocking variables and seek out experimentally fixed effects. This chapter detailed the analytical framework behind the research questions explored in this research. Each research question compelled a specific parametric test and non-parametric test, depending on the data type of the associated variables. The results and implications of the statistical tests are covered in Chapter V.

V. RESULTS

Chapter IV discusses the analytical framework of the research design and data-coding schema that support each primary and ancillary research question assessment. The descriptive statistics for each dependent variable are presented—namely, analyst performance, time, accuracy, confidence, information overload perception, and social impact perception. Chapter IV concludes with controls for identifiable threats to internal and external validity.

This chapter reviews the main and interactive effects that manipulations to the predictor variables (teamwork and ignorance) have on the dependent variables of analyst time, accuracy, performance, confidence, information overload perception, and social impact perception. The research design includes assessments of blocking variables (age, gender, education, and experience) to determine whether demographics have a measurable impact that may explain variation in the dependent variables. This work addresses any possible experimental fixed effect produced by any stimulus scenario that could invalidate the experiment, including the effects of scenario outcomes; Table 14, in Chapter IV, lists 50 supporting research questions, which are answered in this chapter. The nature of each dependent variable, the statistical tests appropriate for each research question, and the effects of predictor variable manipulations are reviewed and effects are interpreted. A summary of the findings in Table 42 concludes the chapter.

Kerlinger and Lee (2000, p. 279) assert that a meaningful way to test a hypothesis is to put it in statistical terms such as “mean A is greater than mean B” at a specified significance level. Following Kerlinger and Lee, this work tested directional hypotheses using one-tailed tests after assessing ancillary research questions with two-tailed tests. Field (2013, p. 539) provides that effect size should accompany significance level. Following Field and Kerlinger and Lee, this research presents statistically significant results along with effect size estimate. Effect size estimate are reported in adjusted R squared for parametric tests and r for nonparametric tests. Nonparametric tests are less powerful but are distribution free and do not require normality assumptions (Kerlinger &

Lee, 2000, p. 415). This research leverages several nonparametric tests to augment the results of parametric tests.

A. ANALYST TIME

Hypotheses 1 and 5 predict that teamwork and ignorance will directionally affect analyst time. Supporting research questions listed in Table 14 (Q4–Q6, Q17, Q18, Q27–Q30) address these hypotheses by investigating the main and interactive effects of ignorance and teamwork with respect to analyst time. Each supporting research question accounts for demographic effects by evaluating blocking variables such as age, gender, education, and experience. The research includes tests for fixed effect by determining whether a scenario or expected outcome had a measurable effect on analyst time.

1. Main Effects

The experimental apparatus recorded time data as number of seconds elapsed from the time the entrance survey was complete to the time the participant initiated a “create case” action. The relationship between the independent and dependent variable levels (categorical and continuous, respectively) indicates that regression and ANOVA are appropriate to determine the difference between means (Kerlinger & Lee, 2000).

a. Ignorance Effects

Hypothesis 1 predicts that a lower level of ignorance will cause higher analyst time. Research question Q6 seeks to determine whether ignorance level significantly affects analyst time. ANOVA ($p < .01$) and regression analysis ($p < .01$) concur that there is a statistically significant difference between analyst time in high- and low-ignorance test groups. The regression analysis in Table 18 reveals a negative relationship between ignorance and time, i.e., as ignorance increases, analyst time decreases.

Table 18. Regression Analysis—Time vs. Ignorance.

Dependent variable: Time

Regression Statistics		
R-Squared (coefficient of determination)		0.4105
Adjusted R-squared		0.3977
Multiple R (multiple correlation coefficient)		0.6407
Standard error of the estimates (SEy)		298.1038
Number of observations		48
Regression Results		
	Intercept	Ignorance
Coefficients	1167.2500	-487.0833
Standard Error	60.8502	86.0551
t-Statistic	19.1824	-5.6601
p-Value	0.0000	0.0000
Lower 5%	1044.7649	-660.3034
Upper 95%	1289.7351	-313.8633

The R^2 statistic reveals that variability in ignorance explains 41% of the variability in analyst time. The nonparametric counterpart for the one-way ANOVA test with two levels is the Mann–Whitney U (1947). The Mann–Whitney U test compares medians rather than means to accommodate outliers in small datasets. The results of the Mann–Whitney U test ($p < .01$) concur with the results of the ANOVA and regression analysis. Table 19 presents the results of this test.

Table 19. Mann–Whitney U Analysis—Time vs. Ignorance.

Test Statistics^a	
	Time
Mann–Whitney U	60.000
Z	-4.701
Asymptomatic	.000
Significance (2-tailed)	

^a Grouping: Ignorance

Although ignorance demonstrates a statistically significant effect, the magnitude of that effect allows comparison with the effects of other variables. The effect magnitude, or size, represents the influence that predictor variable manipulations have on dependent variables. The effect size estimate in Equation 3, r , is calculated using Z score and sample size N (Field, 2013, p. 227). Given sample size N and Z score, effect size is calculated as:

$$r = \frac{Z}{\sqrt{N}}$$

Equation 3. Effect Size Estimate

Following Cohen (1988), Field (2013, p. 82) categorizes effect power as small ($r = .1$), medium ($r = .3$), or large ($r = .5$). In the present experimental manipulation (time vs. ignorance), r is .679 with a negative ignorance correlation coefficient, indicating a large negative effect (low ignorance is coded as 0 and high ignorance as 1). This interpretation subscribes to Field's classification of effect size to provide an objective effect-magnitude elucidation.

Consistent with Hypothesis 1, individuals under conditions of a higher level of ignorance, or lack of information, will complete an ITA task in less time than individuals under conditions of lower ignorance. This finding is intuitive, because those dealing with a greater information-processing demand clearly require more time to process a greater information load. The less intuitive question is how teamwork affects this increase in information-processing load. Theories of specialization and process loss disagree on the time effects of distributing the information-processing load among multiple individuals. The following section demonstrates how teamwork affects analyst time.

b. Teamwork Effects

Hypothesis 5 predicts that teamwork will increase analyst time. Research question Q5 seeks to determine the magnitude and direction of the analyst time effects. ANOVA ($p < .01$) and regression analysis ($p < .01$) concur that there is a statistically significant difference in ITA processing time for those organized into teams or as individuals. The regression analysis in Table 20 reveals a positive relationship between teamwork and time, i.e., as teamwork increases, analyst time increases.

Table 20. Regression Analysis—Time vs. Teamwork.

Dependent variable: Time

Regression Statistics		
R-squared (coefficient of determination)		0.2483
Adjusted R-squared		0.2320
Multiple R (multiple correlation coefficient)		0.4983
Standard error of the estimates (SEy)		336.6283
Number of observations		48
Regression Results		
	Intercept	Teamwork
Coefficients	734.2917	378.8333
Standard Error	68.7140	97.1762
t-Statistic	10.6862	3.8984
p-Value	0.0000	0.0003
Lower 5%	595.9776	183.2278
Upper 95%	872.6057	574.4389

The R^2 statistic reveals that variability in teamwork explains 24% of the variability in analyst time. As stated in the previous section, the nonparametric counterpart for the one-way ANOVA test with two levels is the Mann–Whitney U test. The results of the Mann–Whitney test ($p < .01$) concur with the results of the ANOVA and regression analysis. Table 21 gives the results of the Mann–Whitney U test.

Table 21. Mann–Whitney U Analysis—Time vs. Teamwork.

Test Statistics^a	
	Time
Mann–Whitney U	120.000
Z	-3.464
Asymptomatic	.001
Significance (2-tailed)	

^a Grouping Variable: Teamwork

Teamwork demonstrated a statistically significant effect. As stated previously, the effect size estimate, r , power is categorized as small ($r = .1$), medium ($r = .3$), or large ($r =$

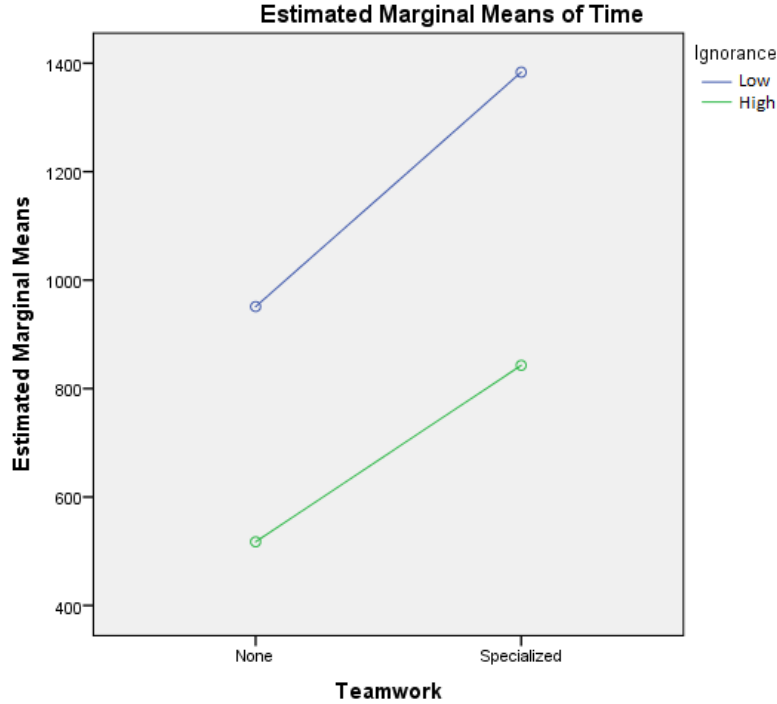
.5). Specific to manipulations of teamwork (time vs. teamwork), r is .500 with a positive teamwork correlation coefficient, indicating a large positive effect. This interpretation is consistent with Field's (2013) interpretation of effect size.

Consistent with Hypothesis 5, individuals organized into horizontally specialized teams took more time to complete an ITA task than those organized individually. This finding is counterintuitive, because those organized into teams had four times the information-processing capacity than those organized as individuals. Furthermore, no debate or group decision making took place, because complete information was restricted to one person on the team, the ITA analyst. References were distributed equally (two each) among participants under both conditions of teamwork. However, results indicate that splitting the work between specialists results in higher analyst time. How much each condition of ignorance affects each condition of teamwork is the focus of the following section.

2. Interactive Effects

Research question Q4 asks whether teamwork and ignorance interact to affect analyst time. ANOVA ($p > .1$) indicates that there is no statistically significant difference in analyst time for those organized into teams under high- or low-ignorance conditions. The lack of interaction between teamwork and ignorance implies that an equal distribution of references between team members has a consistent effect under both conditions of ignorance. The finding also implies that increased references and, consequently, equally distributed additional persons to accommodate the load, will not yield a beneficial effect on analyst time. That is to say, any information-processing benefit realized by distributing the information load incurred a corresponding process loss. This finding is consistent with predictions implied by process-loss theory. The ANOVA results are illustrated in Figure 1.

Figure 1. Interactive Time Effects—Teamwork vs. Ignorance.



3. Blocking Variable Effects

This research evaluates the possible effects of demographics using a blocking technique. Research questions Q27–Q30 investigate the effects of age, gender, education, and experience, respectively, on analyst time. It is possible that chance groupings of certain demographics within certain test groups may create illusory correlations among the independent and dependent variables. Regression analysis indicates no statistically significant relationship between any blocking variables (age, gender, education, or experience) and analyst time. Thus, no variation in analyst time is explicable by age, gender, education, or experience. Regression analysis for the blocking variables is in Appendix E, Section H.

4. Fixed Effects

Research question Q17 investigates the presence of an experimental fixed effect. Properties of an experimental stimulus may have unexpected fixed effects. For instance,

if one scenario generally takes more time to complete than other scenarios, it would be difficult to objectively compare individual performances if the scenario itself accounts for a significant portion of variability in analyst time.

ANOVA is an appropriate test because the independent variable, *Scenario*, is categorical and the order, 1–4, has no significance other than as a label (Kerlinger & Lee, 2000, p. 313). The ANOVA among scenario groups shown in Table 22 suggests that there is no statistically significant analyst time difference ($p > .1$) among each of the four experimental scenarios. The results indicate that no experimentally fixed effect contributed to variability in analyst time.

Table 22. ANOVA Results—Time vs. Scenario.

Tests of Effects Among Subjects					
Dependent Variable: Time					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	548592.083 ^a	3	182864.028	1.260	.300
Intercept	40955380.080	1	40955380.080	282.175	.000
Scenario	548592.083	3	182864.028	1.260	.300
Error	6386239.833	44	145141.814		
Total	47890212.000	48			
Corrected Total	6934831.917	47			

^a R squared = .079 (adjusted R squared = .016)

Analyst time follows a normal distribution, according to the Kolmogorov–Smirnov ($p > .1$) and Shapiro–Wilk ($p > .1$) tests, but fails the homoscedasticity assumption, according to Levene’s test of equality of variances ($p < .05$). This implies that a nonparametric test is more appropriate to compare analyst time among scenarios. The Kruskal–Wallis test is a nonparametric analog for ANOVA with more than two categories (Kerlinger & Lee, 2000, p. 418). The Kruskal–Wallis test results ($p > .1$) concur with the ANOVA results ($p > .1$), indicating that the scenarios are generally equal

with respect to analyst time. Table 23 presents the results from the Kruskal–Wallis test, confirming the results from the ANOVA.

Table 23. Kruskal–Wallis Test—Time vs. Scenario.

Test Statistics ^{a,b}	
	Time
Chi-square	2.342
df	3
Asymptomatic Significance (2- tailed)	.505

^a Kruskal–Wallis test

^b Grouping variable: Scenario

Research question Q18 probes whether the expected scenario outcome (implication vs. exoneration) has a significant effect on analyst time. Two scenarios had an expected implicative outcome and the other two had an expected exonerative outcome. The expected outcomes are similar to suspected guilt vs. innocence, respective to implication vs. exoneration, regardless of intent. Outcome is categorical; thus ANOVA is appropriate for comparing experimental effects among groups. Table 24 reveals that there is no statistically significant difference between scenario outcome and analyst time ($p > .1$). The results suggest that there is no experimentally fixed effect that contributes to variability in analyst time.

Table 24. ANOVA—Time vs. Scenario Outcome.

Tests of Between-Subjects Effects					
Dependent Variable: Time					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected model	206981.333 ^a	1	206981.333	1.415	.240
Intercept	40955380.080	1	40955380.080	280.022	.000
Outcome	206981.333	1	206981.333	1.415	.240
Error	6727850.583	46	146257.621		
Total	47890212.000	48			
Corrected total	6934831.917	47			

^a R squared = .030 (adjusted R squared = .009)

A nonparametric ANOVA equivalent is appropriate because of a homoscedasticity assumption violation revealed by Levene's test of equality of variances ($p < .05$). This implies that a nonparametric test is more appropriate to compare analyst time among scenarios. As noted, the nonparametric counterpart for the one-way ANOVA test with two levels is the Mann–Whitney U test. The results from the Mann–Whitney U test (Table 25) concur with the ANOVA results in Table 24.

Table 25. Mann–Whitney U Analysis—Time vs. Scenario Outcome.

Test Statistics^a	
	Time
Mann–Whitney U	248.000
Z	-.825
Asymptomatic	.409
Significance (2-tailed)	

^a Grouping variable: Outcome

This analysis strongly implies that the scenario and scenario outcome did not contribute to variability in analyst time. Variations in ignorance and teamwork did, however, account for 65.8% of variability in analyst time (.410 and .248, respectively).

This analysis does not account for any accuracy benefits that may manifest at the cost of time. The following section investigates how ignorance and teamwork affect analyst accuracy.

B. ANALYST ACCURACY

Hypotheses 2 and 4 predict that teamwork and ignorance will directionally affect analyst accuracy. The supporting research questions in Table 14 (Q7–Q9, Q21, Q22, Q31–Q34) address these hypotheses by investigating the main and interactive effects of ignorance and teamwork with respect to analyst accuracy. Supporting research questions accounted for any demographic effects by evaluating blocking variables such as age, gender, education, and experience. This work tests for fixed effect by determining whether any scenario or expected outcome had a statistically significant effect on analyst accuracy.

1. Main Effects

Each participant in the four test groups evaluated a single scenario to determine whether an insider was a threat or not. analyst accuracy is coded 0 for incorrect and 1 for correct. The relationship between the predictor and dependent variable levels (which were both categorical) indicates that use of logistic regression is appropriate to determine the difference between means (Kerlinger & Lee, 2000, p. 809).

a. Ignorance Effects

Hypothesis 2 predicts that a higher level of ignorance will cause lower analyst accuracy. Research question Q9 asks whether ignorance level significantly affects analyst accuracy. Regression analysis ($p > .01$) and chi-squared testing ($p > .1$) concur that there is no statistically significant difference in analyst accuracy among high- and low-ignorance test groups. A chi-squared test was appropriate because of the categorical nature of both the predictor and dependent variables (Kerlinger & Lee, 2000, p. 230). The test and regression-analysis results are in Appendix E, Section H. They do not support Hypothesis 2.

b. Teamwork Effects

Hypothesis 4 predicts that teamwork will increase analyst accuracy. Research question Q8 seeks to determine the magnitude and direction of analyst time effects. Logistic-regression analysis ($p < .1$) and chi-squared testing ($p < .1$) concur that there is a small but statistically significant difference in analyst accuracy for those organized into teams vs. individuals. The regression analysis in Table 26 reveals a small positive relationship between teamwork and accuracy, i.e., teams are slightly more accurate than individuals.

Table 26. Logistic Regression Analysis—Accuracy vs. Teamwork.

Dependent Variable: Accuracy					
Regression Results					
Log Likelihood	Value	27.1141	Approach	Logit	
	Variable	Coefficients	Standard Error	Z-Statistic	p-Value
		0.3367	0.4140	0.8133	0.4161
	Teamwork	1.2726	0.6866	1.8535	0.0638

Consistent with other findings in this dissertation, I use nonparametric tests to confirm results from parametric tests. A parametric analog for logistic regression with categorical predictor and dependent variables is the chi-squared test. Table 27 presents the results of the chi-squared test.

Table 27. Chi-Squared Test—Accuracy vs. Teamwork.

Chi-Square Tests					
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2- sided)	Exact Sig. (1-sided)
Pearson chi-square	3.630 ^a	1	.057		
Continuity correction	2.521	1	.112		
Likelihood ratio	3.721	1	.054		
Fisher's exact test				.111	.055
Linear-by-linear association	3.555	1	.059		
N of valid cases	48				

The effect magnitude, or size, represents the influence that predictor variable manipulations have on dependent variables. Phi is a measure of the strength of association among variables in a chi-squared test. Phi (φ) is calculated using a chi-squared (X^2) score and sample size n (Field, 2013, p. 740). Given n and X^2 , effect size is calculated in Equation 4 as:

$$\varphi = \sqrt{\frac{X^2}{n}}$$

Equation 4. Phi

Following Cohen (1988), Field (2013, p. 82) categorizes effect power as small ($\varphi = .1$), medium ($\varphi = .3$) and large ($\varphi = .5$). In the present experimental manipulation (analyst time vs. ignorance), φ is .275, indicating a small effect. The crosstab in Table 28 shows the relationship between teamwork and accuracy.

Table 28. Cross Tabulation—Accuracy vs. Teamwork.

		Teamwork		Total
		None	Specialized	
Accuracy	Incorrect	10 (41.6%)	4 (16.6%)	14
	Correct	14 (58.3%)	20 (83.3%)	34
Total		24	24	48

Individuals who performed ITA while organized into teams were more accurate than those organized as individuals—83% vs. 58% respectively, a difference of 25%. Supporting Hypothesis 4, the results indicate that ITA analysts organized into teams perform with greater accuracy than those organized individually.

2. Interactive Effects

Research question Q7 asks whether teamwork and ignorance interact to affect analyst accuracy. ANOVA ($p > .1$) indicates that there is no statistically significant interaction between ignorance and teamwork that affects analyst accuracy. The ANOVA results supporting Q7 are found in Appendix E.

3. Blocking Variable Effects

Research questions Q31–Q34 investigate the effects of age, gender, education, and experience on analyst accuracy. Owing to the low sample size, chance groupings of participants that have specific demographic characteristics may contribute to some variability in analyst accuracy, leading to illusory correlations. The regression analysis in Table 29 indicates a small relationship between gender and analyst accuracy ($p < .1$).

Table 29. Logistic Regression Analysis—Accuracy vs. Age, Gender, Education, and Experience.

Dependent Variable: Accuracy

Regression Results				
Log Likelihood Value	-25.586	Approach	Logit	
Variable	Coefficients	Standard Error	Z-Statistic	p-Value
	0.4870	1.3146	0.3704	0.7111
Age	-0.0557	0.0358	-1.5542	0.1201
Gender	1.3960	0.7897	1.7678	0.0771
Education	1.0282	0.6753	1.5227	0.1278
Experience	-0.0241	0.0679	-0.3551	0.7225

Research question Q32 specifically addresses the relationship between analyst accuracy and gender by removing all noise variables to test the specific relationship. The logistic regression results in Table 30 suggest no statistically significant relationship between gender and analyst accuracy. As a result, the findings indicate that the selected demographics had no effect on analyst accuracy.

Table 30. Logistic Regression Analysis—Accuracy vs. Gender.

Results				
Log Likelihood Value	-27.7332	Approach	Logit	
Variable	Coefficients	Standard Error	Z-Statistic	p-Value
	0.0018	0.6325	0.0029	0.9977
Gender	1.1673	0.7386	1.5805	0.1140

4. Fixed Effects

This research produced some unexpected findings as to how scenario outcomes affect analyst accuracy. Research question Q21 investigates whether an experimental fixed effect is present. The experimental stimulus may explain some of the variability in analyst accuracy. For instance, if a specific scenario is more likely to result in a correct

answer, it would be difficult to compare individual performance objectively, because the scenario itself would explain a significant portion of variability in analyst accuracy.

Table 31. Cross Tabulation—Accuracy vs. Scenario.

		Scenario (Expected Outcome)				Total
		1 (Exonerate)	2 (Implicate)	3 (Exonerate)	4 (Implicate)	
Accuracy	Incorrect	5 (41.6%)	0 (0%)	5 (41.6%)	4 (33.3%)	14 (29.1%)
	Correct	7 (58.3%)	12 (100%)	7 (58.3%)	8 (66.6%)	34 (70.9%)
Total		12	12	12	12	48

Scenario 2 was the only scenario describing a malicious insider threat. The remaining scenario accuracy scores were more evenly distributed. Those assigned to the four experimental groups evaluated Scenario 2 three times, and all twelve responded correctly each time—so the accuracy effect is equal across all experimental groups. Thus, there is no chance that experimental bias threatened the validity of the analyst accuracy score among experimental groups.

Research question Q22 investigates the possible effects of scenario outcome. With exonerative outcomes coded 0 and implicative outcomes, 1, logistic regression

indicates that scenario outcome has an effect on analyst accuracy. According to the logistic regression in Table 32, there is a small, statistically significant scenario-outcome effect ($p < .1$).

Table 32. Regression Analysis—Scenario Outcome vs. Accuracy.

Dependent Variable: Accuracy				
Results				
Log Likelihood	Value	-27.1141	Approach	Logit
Variable	Coefficients	Standard Error	Z-Statistic	p-Value
Scenario	0.3367	0.4140	0.8133	0.4161
Outcome	1.2726	0.6866	1.8535	0.0638

A chi-squared test under the same conditions concurs that scenario outcome has a small significant effect ($p < .1$). The magnitude of the effect was also small ($\phi = .275$), indicating that scenario outcome (exoneration or implication) had a small effect on accuracy. The results from the chi-square test are in Appendix E, Section H. Participants were more likely to interpret implicative scenarios correctly over exonerative scenarios. However, this finding is affected by Scenario 2 fixed effects, in which participants correctly implicated the suspect in all twelve trials. Table 33 provides a cross tabulation of analyst accuracy vs. scenario outcome.

Table 33. Cross Tabulation—Accuracy vs. Scenario Outcome.

		Expected Outcome		
		Exonerate	Implicate	Total
Accuracy	Incorrect	10 (41.7%)	4 (16.7%)	14 (29.2%)
	Correct	14 (58.3%)	20 (83.3%)	34 (70.8%)
Total		24	24	48

Participants assessed exonerative scenarios with 58% accuracy, but implicative scenarios with 83% accuracy, a difference of 25%. This is interesting because participants were marginally better than chance when performing a threat assessment on an innocent person, but far better at identifying a true insider threat. Furthermore, all participants obtained express instructions that they were not to err on the side of caution, because an incorrect response would cost them the Silver Eagle prize. All participants were equipped with adjudicative guidelines and current on mandatory insider threat training, yet implicated an innocent person in 41.7% of trials.

The experimental data suggests teamwork causes higher accuracy, but this boost comes at the cost of time. ITA teams require, on average, 65% more time assessing insider threats than individuals under the same conditions of ignorance. The following section combines analyst accuracy and time into a single performance measure for an objective comparison of the experimental groups.

C. ANALYST PERFORMANCE

Taken together, the experimental support for hypotheses 4 and 5 indicates that teamwork increases analyst accuracy, at the cost of time. Following Jaquith (2009), this dissertation defines performance as accuracy within a certain time. Supporting research questions listed in Table 14 (Q1–Q3, Q19, Q20, Q35–Q38) seek to inform which experimental condition provides the greatest analyst performance. Table 34 presents descriptive statistics for each experimental group. The data that informed Table 34 is in Appendix E (A).

Table 34. Descriptive Statistics—Time, Accuracy, and Performance.

		Ignorance	
Teamwork	Specialized	High	Low
		Time	Time
		Mean: 842.83	Mean: 1383.41
		Median: 805.5	Median: 1277
	None	Score: 58.3%	Score: 31.5%
		Accuracy: 75%	Accuracy: 91%
		Performance: 66.6%	Performance: 61%
		Time	Time
		Mean: 517.5	Mean: 951.08
		Median: 501.5	Median: 842
		Score: 74.4%	Score: 52%
		Accuracy: 74%	Accuracy: 66%
		Performance: 62.2%	Performance: 59.8%

The chart indicates that analysts under conditions of no teamwork and high ignorance resulted in the best time, but analysts under conditions of teamwork and low ignorance resulted in highest accuracy. Analysts under conditions of both teamwork and high ignorance, however, resulted in the highest performance. The results combined into a single performance metric were not as significant, because there was little variability in analyst performance among the experimental groups.

The research questions also address any interactive effects of ignorance and teamwork on analyst performance. The supporting research questions account for demographic effects by blocking variables that include age, gender, education, and experience. The research included tests for fixed effect by determining if any scenario or expected outcome had a measurable effect on analyst performance.

1. Main Effects

As discussed in Chapter IV, accuracy and the time required to perform ITA together define analyst performance. Analyst performance scores range along a continuum from 0 to 2; participants who take no time to get the correct answer receive a 2 and he who takes the longest time to get an incorrect answer receives a 0. The nature of the predictor and dependent variables (categorical and ratio, respectively) indicate that

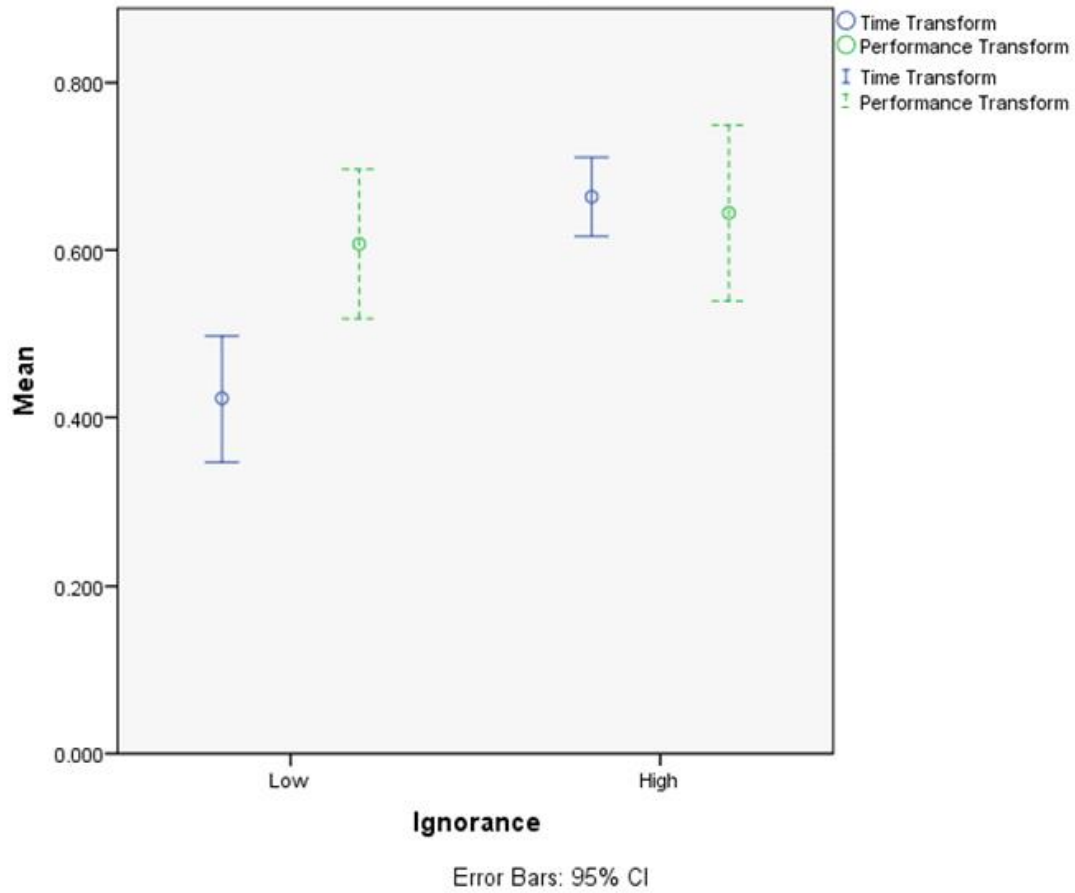
ANOVA and regression analysis are appropriate statistical analysis methods (Kerlinger & Lee, 2000).

a. Ignorance Effects

Research question Q3 investigates how ignorance affects performance. Ignorance had a large effect on analyst time, but no significant effect on accuracy. Regression analysis reveals no significant difference in performance between the conditions of ignorance ($p > .1$), while the Mann–Whitney U test reveals a slightly significant difference ($p < .1$). The effect magnitude ($r = -.23$) indicates a small negative effect between ignorance and performance. Low ignorance is coded 0 and high ignorance, 1. Note that accuracy was relatively unchanged by either condition of ignorance, so the relationship between performance and ignorance is best explained by the magnitude of the relationship between analyst time and ignorance, as discussed previously.

Field (2013, p. 379) emphasizes the importance of error bars for visualizing differences among dependent variables under various experimental conditions. I transform both the analyst time and performance scores to a scale from 0 to 1. The transform presents lower analyst time as a higher time score and, similarly, higher performance results in a higher performance score. The error bar chart in Figure 2 illustrates the 95% confidence intervals around the means of analyst time and performance transforms, relative to the two conditions of ignorance.

Figure 2. Error Bar Chart—Time and Performance vs. Ignorance.



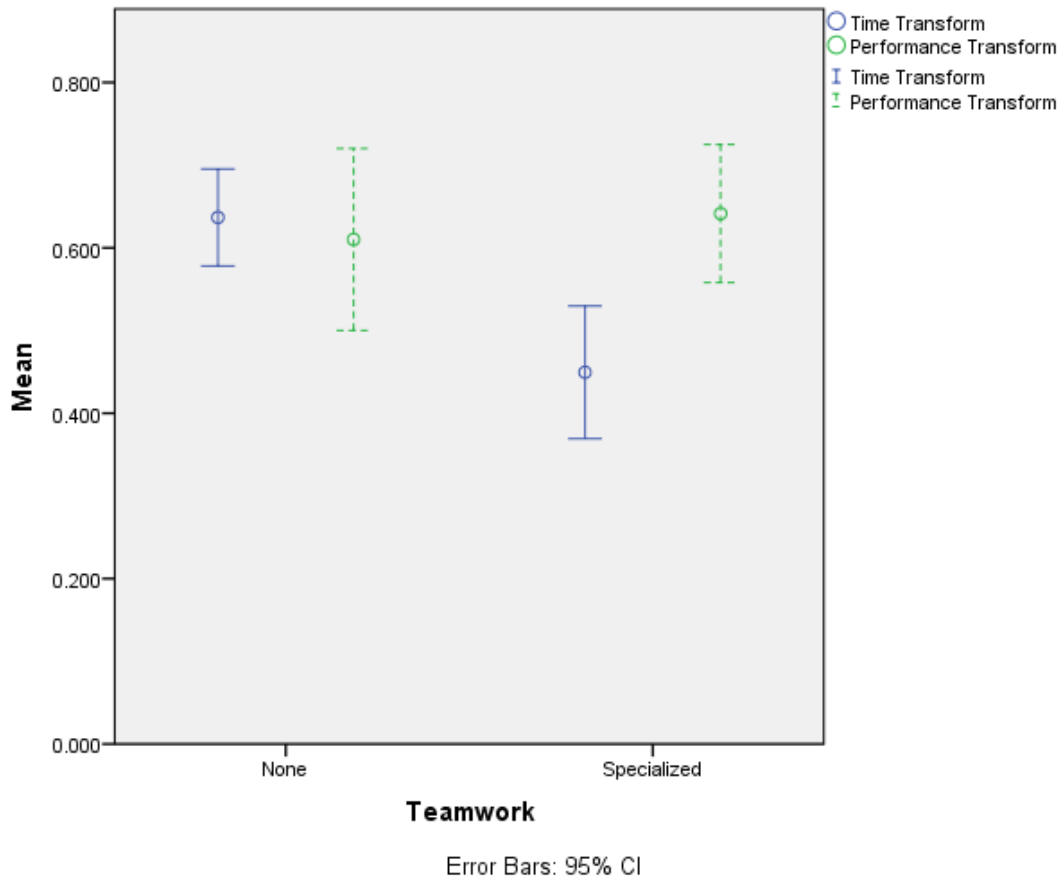
The error bars in Figure 2 suggest that whatever time benefits (solid lines) that conditions of high ignorance produced came at a nearly equivalent cost of accuracy. Likewise, whatever accuracy benefit low ignorance produced came at a nearly equivalent cost of time. As a result, performance (dotted lines) under both conditions was relatively unchanged.

b. Teamwork Effects

Research question Q2 investigates how teamwork affects performance. Teamwork had a small effect on accuracy and a large effect on analyst time. However, regression analysis and Mann–Whitney U reveal no significant difference in analyst performance between the two conditions of teamwork ($p > .1$). The results of the analysis are given in Appendix B. Using the same time and performance transform discussed in

the previous section, Figure 3 presents the 95% confidence intervals around the means of analyst time and performance transforms, relative to the two conditions of teamwork.

Figure 3. Error Bar Chart—Time and Performance vs. Teamwork.



The error bars in Figure 3 suggest that whatever time benefits (solid lines) that conditions of no teamwork produced came at a nearly equivalent cost of accuracy. Similarly, whatever accuracy benefit specialized teamwork produced came at a nearly equivalent cost of time. As a result, performance (dotted lines) under both conditions was relatively unchanged.

2. Interactive Effects

Research question Q1 seeks to determine whether teamwork and ignorance interact to affect analyst performance. ANOVA ($p > .1$) indicates that there is no

statistically significant interaction between ignorance and teamwork that affected analyst performance. The ANOVA results that support Q1 are in Appendix E. The results were as expected, since there were negligible analyst performance effects under either condition of teamwork and either condition of ignorance.

3. Blocking Variable Effects

Research questions Q35–Q38 investigate whether demographics affect analyst performance. Consistent with the findings from regressions in the previous two sections, demographics had no effect on analyst performance ($p > .1$). The results from the regression analysis are in Appendix B.

4. Fixed Effects

Research question Q19 investigates whether an experimental fixed effect is present in the scenario stimulus. According to regression analysis, scenario has no effect on performance ($p > .1$). However, a Kruskal–Wallis test revealed a statistically significant difference in analyst performance among scenarios ($p < .1$) and a medium effect size ($\phi = .381$). The previously noted fixed effect with Scenario 2 and the planned correlation between analyst accuracy and performance explains the small performance effect. As stated previously, the accuracy effect is equal across all experimental groups. Thus, no experimental bias threatened the validity of the analyst performance score among experimental groups. Table 35 presents the results of the Kruskal–Wallis test, showing a marginally significant difference among scenarios.

Table 35. Kruskal–Wallis Test—Scenario vs. Performance.

Test Statistics ^{a,b}	
	Performance
Chi-square	6.975
df	3
Asymp. sig.	.073

^a Kruskal Wallis Test

^b Grouping variable: Scenario

Research question Q20 tests the effect that expected outcome has on analyst performance. It is interesting to note that the scenario fixed effect was not present in a similar test of scenario outcome. ANOVA ($p > .1$), regression ($p > .1$), and Mann–Whitney U ($p > .1$) analysis concur that performance is generally the same among implicative- and exonerative-outcome groups.

D. INFORMATION OVERLOAD PERCEPTION

Hypothesis 7 predicts that teamwork and ignorance will interact to affect the perception of information overload. Supporting research questions listed in Table 14 (Q13–Q15, Q25, Q26, Q43–Q46) address this hypothesis by investigating the main and interactive effects of ignorance and teamwork with respect to the perception of information overload. The supporting research questions account for any demographic effects by evaluating blocking variables such as age, gender, education, and experience. This research tests for fixed effect by determining whether each scenario or expected outcome has a statistically significant effect on the perception of information overload.

This work did not limit the time available for ITA, so if Shick et al. (1990) are correct, perceptions of information overload should remain unchanged when the information load increases, but is evenly distributed among additional people. Chewing and Harrell's (1990) cuing theory posits that the cues within information processed simultaneously will affect information overload, regardless of time constraints. ANOVA is useful for evaluating interactive effects.

1. Main Effects

The experimental apparatus recorded the perception of information overload by means of a web survey presented to each participant at the conclusion of ITA. The survey is adapted from Soucek & Moser (2010). Survey items measure information overload on a nine-point scale with 1 representing no information overload and 9 representing high information overload. This research does not include main-effects hypotheses, because it is well documented and intuitive principle that more information will result in higher perceptions of information overload, all else being equal. Hypothesis 1 produced

convincing confirmatory evidence because of the analyst time increase that accompanied information increases.

a. Ignorance Effects

Research question Q15 asks whether information-overload perceptions increase as information increases under conditions of unlimited time. Schick's (1990) temporal approach to information overload predicts it will not. Chewing and Harrell's (1990) cueing approach, however, argues that the number of cues is an information-overload factor. If Chewing and Harrell are right, the results should demonstrate an increased perception of information overload under conditions of low ignorance. (Recall that low-ignorance participants were required to process twice the number of references as high-ignorance participants.)

Results from both regression ($p > .1$) and Mann–Whitney U ($p > .1$) concur that there is no statistically significant difference in the perception of information overload between groups of high and low ignorance (see test results in Appendix E). The test results strongly indicate that a time constraint is a necessary component for the perception of information overload, supporting Schick's temporal approach.

b. Teamwork Effects

Research question Q14 answers the question, “does coordination overhead contribute to perceptions of information overload?” Steiner's (1972) work on process-loss theory predicts that the “coordination links” between people in a communicating system will contribute to process loss. The present test seeks to determine whether the coordination overhead contributes to a perception of information overload.

Results from both regression ($p > .1$) and Mann–Whitney U ($p > .1$) concur that there is no statistically significant difference in the perception of information overload between teamwork conditions.

2. Interactive Effects

Research question Q13 investigates the interactive effects that teamwork and ignorance have on perceptions of information overload. ANOVA indicates a significant interaction ($p < .1$) between ignorance and teamwork affecting the perception of information overload. Table 36 presents the results of the test.

Table 36. ANOVA Results—Teamwork vs. Ignorance per Information Overload.

Tests of Effects Among Subjects								
Dependent Variable: InfoOvld								
Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power ^b
Corrected Model	6.563 ^a	3	2.188	1.652	.191	.101	4.957	.403
Intercept	180.188	1	180.188	136.107	.000	.756	136.107	1.000
Teamwork	.188	1	.188	.142	.708	.003	.142	.066
Ignorance	1.688	1	1.688	1.275	.265	.028	1.275	.197
Teamwork * Ignorance	4.688	1	4.688	3.541	.067	.074	3.541	.453
Error	58.250	44	1.324					
Total	245.000	48						
Corrected Total	64.813	47						

^a R squared = .101 (adjusted R squared = .040)

^b Computed using alpha = .05

I leverage a bootstrap simulation technique to provide statistical sampling, exploiting the computational capacity of software (Law & Kelton, 1991). Nonparametric bootstrap simulation gives the data statistical power to use ANOVA to present interactive effects. Nonparametric bootstrap simulation is a nonparametric analog to Monte Carlo simulation (Mun, 2015, p. 94).

Using Risk Simulator (Mun, 2015), I performed a nonparametric bootstrap simulation with 100 trials per test condition (400 additional trials) with seed value set to 1. The simulation results meet the normality assumption because “if the size of the sample, n , is sufficiently large (no less than thirty; preferably no less than 50), then the central limit theorem will apply, even if the population is not normally distributed along variable x ” (Sirkin, 1999, p. 245). The central limit theorem states, “if samples are drawn from a population at random, the means of the samples will tend to be normally distributed” (Kerlinger & Lee, 2000, p. 286).

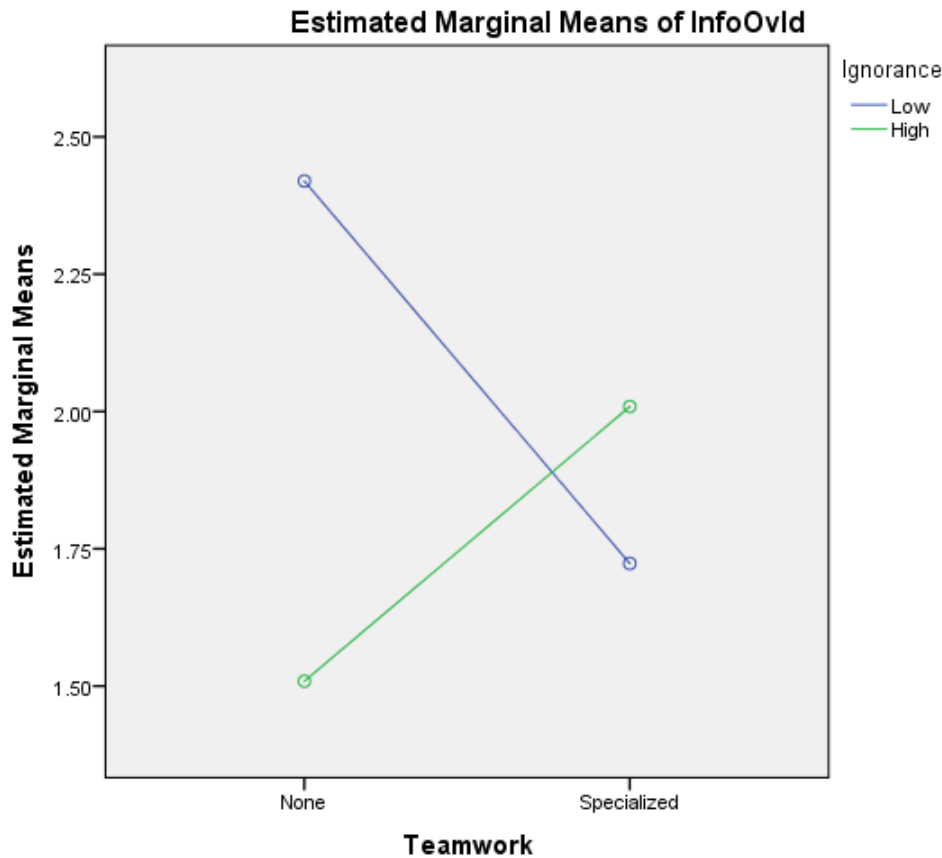
The findings of an ANOVA on the simulated data concur with the results from the ANOVA performed on the original dataset. The ANOVA results using simulated data reveal a statistically significant interaction between ignorance and teamwork ($f = 30.75$, $p < .01$). The results of the ANOVA based on bootstrap simulation data are found in Appendix E, Section H. Field (2013, p. 473) stress that partial eta squared as shown in the SPSS ANOVA output is slightly biased and recommend omega squared (ω^2) as the appropriate effect-size measure. Equation 5 is the omega-squared calculation formula, such that MS is mean square, df is degree of freedom, and SS is sum of squares.

$$\omega^2 = \frac{df_{effect}(MS_{effect} - MS_{error})}{SS_{total} + MS_{error}}$$

Equation 5. Omega-Squared Calculation Formula

According to Field (2013, p.474), the ω^2 values of .01, .06, and .14 are small, medium, and large, respectively. The interaction between ignorance and teamwork demonstrated a small effect size ($\omega^2 = .017$) respective to Field’s interpretation. This finding supports Hypothesis 7. Figure 4 depicts the interaction between teamwork and ignorance.

Figure 4. Interactive Information Overload Effects—Teamwork vs. Ignorance.



The interaction between teamwork and ignorance is best explained by variation in the number of persons used to distribute the information load under each condition of teamwork. In an effort to create a fair test between conditions of teamwork, participants were limited to two references each. As a result, participants under conditions of low ignorance and no teamwork evaluated eight references each and participants under conditions of low ignorance and horizontally specialized teamwork evaluated two references each. Teammates processed the remaining references, at two per person. The decreased perception of information overload under these conditions is intuitive.

Conditions of high ignorance, however, resulted in the opposite effect. Participants assigned high ignorance processed four references when not assigned

teamwork and two references when assigned teamwork. It is counterintuitive that perceptions of information overload should increase when information-processing demands are halved. Yet this perception increased above the perception of information overload for those who were assigned teamwork and collectively processed twice as many references. One possible explanation is the Ringlemann effect, which I measured as the perception of social impact. I test for variability in social impact in Section F.

3. Blocking Variable Effects

Research questions Q43–Q46 investigate whether demographics have an effect on the perception of information overload. Consistent with the findings from regressions in the previous three sections, demographics had no effect on analyst performance ($p > .1$). The results from the regression analysis are in Appendix B (E).

4. Fixed Effects

Research question Q25 asks whether an experimental fixed effect is present in the scenario stimulus. Regression analysis ($p > .1$) and the Kruskal–Wallis test ($p > .1$) concur that scenario had no effect on performance. Similarly, Q26 investigates whether scenario outcome has any effect on the perception of information overload, and regression analysis ($p > .1$) and the Mann–Whitney U test ($p > .1$) concur it has none. The following section investigates whether perceptions of social impact explain some of the interaction between teamwork and ignorance.

E. SOCIAL-IMPACT PERCEPTION

Hypothesis 8 predicts that a lower level of ignorance will cause higher perceptions of social impact. The supporting research questions in Table 14 (Q16, Q47–Q50) seek to inform as to which experimental condition provides the greatest analyst performance. The experimental apparatus recorded the perception of social impact from those organized into teams via a web survey presented to each participant at the conclusion of ITA. The survey instrument for perception of social impact derives from Mulvey & Klein’s (1998) work on collective efficacy and group process and performance. The survey item measures the perception of a negative social impact on a

nine-point scale, with 1 representing no negative social impact and 9 representing high negative social impact.

1. Main Effects

The social impact survey item specifically states “I rushed through the task because I was considerate of my teammates’ time” and asks how much each participant agrees. I leveraged no additional survey items to measure how each participant evaluated his teammates’ social impact, because such an evaluation is subjective by nature and the participant cannot measure how a teammate truly feels. Instead, I focused on how the participant perceived social impacts relative to himself.

Research question Q16 poses the question “does ignorance affect perceptions of social impact?” Results from both ANOVA ($p > .1$) and Mann–Whitney U ($p > .1$) concur that there is no statistically significant difference in the perception of social impact under either condition of ignorance. The statistical results are in Appendix B. Thus, there is no support for Hypothesis 8. This assessment did not include social-impact effects under conditions of no teamwork, because some participants performed ITA under conditions of no teamwork, as individuals; thus, no social impact was possible.

2. Blocking Variable Effects

Research questions Q47–Q50 probe the effects of demographics on perceived social impact. Regression analysis indicates that there is no relationship between demographics and social impact ($p > .1$). The results of the regression analysis are provided in Appendix B.

F. CONFIDENCE

Analyst confidence is a measure roughly analogous to the tendency to guess during ITA. The assumption is that the assessments of participants who are not confident in their ITA are no better than chance. Hypotheses 3 and 6 predict that teamwork and ignorance will directionally affect analyst confidence. Supporting research questions listed in Table 14 (Q10–Q12, Q23, Q24, Q39–Q42) address these hypotheses by investigating the main and interactive effects of ignorance and teamwork with respect to

analyst confidence. Supporting research questions accounted for any demographic effects by evaluating blocking variables such as age, gender, education, and experience. The research includes tests for fixed effect by determining if each scenario or expected outcome affected analyst confidence.

1. Main Effects

The experimental apparatus recorded analyst confidence with a web survey presented to each participant at the conclusion of ITA. The confidence survey asks the participant how much he agrees with the statement “I feel confident that my threat assessment is correct.” The survey item measures the response on a nine-point scale, with 1 representing low confidence and 9 representing high confidence.

a. Ignorance Effects

Research question Q12 investigates whether ignorance affects analyst confidence. Results from both regression ($p > .1$) and Mann–Whitney U ($p > .1$) concur that there is no statistically significant difference in analyst confidence based on condition of ignorance. The statistical results are in Appendix B, showing that Q12 does not support Hypothesis 3.

b. Teamwork Effects

Research question Q11 asks how teamwork affects analyst confidence. Results from both regression ($p > .1$) and Mann–Whitney U ($p > .1$) concur that there is no statistically significant difference in analyst confidence based on condition of teamwork. The statistical results are in Appendix B. Research question Q11 offers no support for Hypothesis 6.

2. Interactive Effects

Research question Q10 tests whether teamwork and ignorance interactively affect analyst confidence. ANOVA results suggest there is no evidence of interaction between teamwork and ignorance ($p > .1$). The statistical results are in Appendix E.

3. Blocking Variable Effects

Research questions Q39–Q42 evaluate how demographics affect analyst confidence. analyst confidence is the only dependent variable for which the statistical tests provided evidence suggesting an effect. The regression analysis in Table 37 indicates that education level has a moderately significant positive effect on analyst confidence ($p < .5$). The results from a regression analysis model specifically addressing the relationship between education and analyst confidence are in Appendix E, Section H.

Table 37. Regression Analysis—Analyst Confidence vs. Age, Gender, Education, and Experience.

Dependent Variable: Confidence					
Regression Statistics					
R-squared (coefficient of determination)	0.1359				
Adjusted R-squared	0.0555				
Multiple R (multiple correlation coefficient)	0.3686				
Standard error of the estimates (SEy)	1.1575				
Number of observations	48				
Regression Results					
	Intercept	Age	Gender	Education	Experience
Coefficients	6.5898	-0.0167	0.0153	0.7489	0.0322
Standard Error	0.7211	0.0179	0.4216	0.3097	0.0306
t-Statistic	9.1383	-0.9299	0.0362	2.4179	1.0492
p-Value	0.0000	0.3576	0.9713	0.0199	0.3000
Lower 5%	5.1355	-0.0528	-0.8349	0.1243	-0.0297
Upper 95%	8.0441	0.0195	0.8654	1.3735	0.0940

The correlation's statistical significance may be partly explained by the disproportionate number of participants who held bachelor's and master's degrees, relative to those with doctorates and postdoctoral degrees. To account for this, I evaluate the effect size with Cohen's f^2 formula, presented in Equation 6.

$$f^2 = \frac{R^2}{1 - R^2}$$

Equation 6. Cohen's f^2 Formula

Following Cohen's (1988, p. 74) guidelines, f^2 effect sizes of .1, .25, and .5 are small to medium, medium to large, and very large, respectively. Regression analysis thus indicates that education has a small effect on analyst confidence ($f^2 = .1572$). The Kruskal–Wallis test did not concur with the regression-analysis results and suggests that education had no effect on analyst confidence ($p > .1$). The results of the Kruskal–Wallis test are in Appendix E, Section H.

4. Fixed Effects

Recall the substantial effect that scenario had on accuracy, specifically, scenario outcome. Participants performing ITA were generally more accurate in implicative than exonerative scenarios. Research questions Q23 and Q24 evaluate how confident participants were in performing ITA on each scenario and assess differences in analyst confidence among scenario outcomes. The research questions seek to explain why analyst accuracy was not much better than chance when participants were presented scenarios with exoneration outcomes. Research question Q21 and Q22 provided evidence that an experimental fixed effect is present in exonerative scenarios. If accuracy was not much better than chance, owing to guesswork, then confidence should be significantly lower in exoneration-scenario outcomes than implicative scenario.

Research question Q23 seeks to determine whether analyst confidence significantly differed between scenarios. Regression is an appropriate test because the independent variable, scenario, is categorical and the dependent variable, analyst confidence, is ordinal. The regression results suggest no statistically significant analyst accuracy difference ($p > .1$) among the four experimental scenarios. The results from the logistic regression did not concur with results from a Kruskal–Wallis test under the same conditions of analyst confidence and scenario. The Kruskal–Wallis test indicates a large ($p < .01$) difference between groups. The regression result is in Appendix E, Section H; Table 38 presents the Kruskal–Wallis test result.

Table 38. Kruskal-Wallis Test—Confidence vs. Scenario.

Test Statistics ^{a,b}	
Confidence	
Chi-Square	12.123
df	3
Asymp. Sig.	.007

^aKruskal Wallis Test

^bGrouping Variable: Scenario

The test results indicate that scenario had a large effect on analyst confidence (ϕ .502), implying that participants were not equally confident across all scenarios. As established previously, scenario outcome had a small effect on analyst accuracy, such that those performing ITA scenarios with an exonerative outcome were generally less accurate than those performing ITA on implicative scenarios.

Research question Q24 investigates how scenario outcome affects analyst confidence. Regression analysis reveals a significant correlation between analyst confidence and scenario outcome ($p < .01$). Table 39 presents the results of the regression.

Table 39. Regression Analysis—Confidence vs. Scenario Outcome.

Regression Statistics		
R-Squared (Coefficient of Determination)	0.2813	
Adjusted R-Squared	0.2656	
Multiple R (Multiple Correlation Coefficient)	0.5303	
Standard Error of the Estimates (SEy)	1.0206	
Number of Observations	48	
Regression Results		
	Intercept	Outcome
Coefficients	6.5417	1.2500
Standard error	0.2083	0.2946
t-statistic	31.4000	4.2426
p-value	0.0000	0.0001
Lower 5%	6.1223	0.6569
Upper 95%	6.9610	1.8431

The Mann–Whitney U results in Table 40 strongly suggest a positive relationship between scenario outcome and analyst confidence ($p < .01$). Recall that the exonerative scenario outcomes are coded 0 and implicative scenario outcomes are coded 1. Mann–Whitney and regression analysis concur that participants are more likely to be confident with their assessment when evaluating implicative scenarios than exonerative scenarios. Following Cohen’s (1988) guidelines, the effect size was medium ($\phi = .499$).

Table 40. Mann–Whitney Test—Confidence vs. Scenario Outcome.

Test Statistics ^a	
	Confidence
Mann–Whitney U	125.500
Z	-3.463
Asymp. Sig. (2-tailed)	.001

^aGrouping Variable: Outcome

The findings strongly suggest that participants were more likely to guess when presented an exonerative outcome than an implicative outcome. Recall that the analyst accuracy test results indicated that participants who performed ITA on exonerative scenarios achieved little better than chance. The scenario-outcome test results strongly suggest that participants were more likely to be little better than chance with exonerative scenarios because they were more likely to guess in such a case.

Taken all together, participants did little better than chance when performing ITA on exonerative outcomes. Although it was not in the original research design, an evaluation of which conditions are best for analyst accuracy, specific to exonerations, is offered. Lacking sufficient sample size for predictive statistics, I use descriptive statistics to evaluate the relationship between teamwork and accuracy. Participants organized as individuals under high- and low-ignorance conditions were, on average, 33% and 50% accurate, respectively. Those organized in specialized teams under high- and low-ignorance conditions were, on average, 66% and 83% accurate, respectively. Thus, individuals organized in specialized teams were better than chance at ITA when limited

to exonerative outcomes. In other words, higher ignorance resulted in greater likelihood of implicating an innocent than exonerating a genuinely threatening insider.

G. DISCUSSION

This chapter reviews the statistical evidence suggesting that the accuracy and promptitude of insider threat analysts are controllable by varying the structure of teamwork to accommodate the level of ignorance specific to environmental constraints. In support of Hypothesis 4, participants organized in specialized teams were marginally more accurate than those organized as individuals ($Z=1.853$, $p=.063$, $r=.267$; $X^2 = 3.63$, $p = .057$, $\phi = .275$). This boost in accuracy however, came at a cost in time. Planned contrasts strongly support Hypothesis 5, indicating that organizing participants into specialized teams significantly increases the time of ITA compared to participants working individually ($F(1,46)=15.198$, $p=.000$, $R^2_{adj}=.232$; $U = 67.5$, $p = .001$, $r = .679$). The evidence strongly supports Steiner's process-loss theory as it applies to insider threat analysis.

I introduce a metric for ITA that evaluates performance as a function of accuracy within a given period of time. The performance score evaluated participants benchmarked off each other, but did not reveal a statistically significant difference between groups. The results concur with the NITTF conclusion that small ITA programs with minimal budget can perform as well as large, well-funded programs. This experiment demonstrates how that counterintuitive observation is possible.

Recall that there was no group decision making because only one person, the insider threat analyst, had all the information needed to make a decision and could not discuss this information with the team. Furthermore, information was specific to each team member, so there was no information-processing redundancy. Regardless, individuals with the same information consistently outperformed teams in analyst time, at the expense of accuracy. Whereas participants performed ITA with no time limit, according to Simon's theory of bounded rationality, people naturally operate within temporal constraints. Depending on environmental time constraints, information overload will increase (Schick et al., 1990) and become a problem for proper ITA (Cappelli, et al.,

2012, p. 196; Garst & Gross, 1997), implying increased misattributions or lower analyst accuracy.

Teamwork and ignorance interactively affected the perception of information overload, according to the participants. Planned contrasts using simulated data revealed an interaction between ignorance and teamwork ($F(1,44)=3.541$, $p=.067$, $R^2_{adj}=.040$; $F(1,444)=30.752$, $p=.000$, $R^2_{adj}=.076$) that affected perceptions of information overload. The results suggest that specialized teamwork decreases information overload perception in low-ignorance environments, but increases the information-overload perception in high-ignorance environments. The results are consistent with Tushman and Nadler's (1979) theory of organizations as information processors and supports Hypothesis 7. This research indicates that varying conditions of information and organization can result in more optimal ITA, depending on the measure of interest, accuracy, or promptitude.

Tests intended to validate the equality of the scenario stimulus produced some unexpected results with strong implications for ITA. The scenario outcome (i.e., exoneration or implication) strongly affect accuracy. The findings indicate that participants are fairly accurate when evaluating an implicative scenario but perform little better than chance in an exonerative scenario. Participants organized in teams under conditions of high and low ignorance resulted in considerably higher accuracy (.66 and .83, respectively) than participants organized as individuals (.33 and .5, respectfully) when performing ITA on an exonerative scenario. This boost in accuracy came at a time cost similar to that of implicative scenarios. I predict time from the regression equation in Equation 7 such that $Y = \text{ITA time prediction}$, $a = \text{intercept}$, b_i is the beta coefficient of each predictor variable, and X_i is the value of each predictor variable.

$$Y = a + b_1X_1 + b_2X_2 + b_3X_3$$

Equation 7. Regression Equation

The predictions per scenario outcome indicate that participants take less time to evaluate exonerative scenarios and participants organized as individuals are no better than chance at ITA with exonerative scenarios. However, specialized teams are better

than chance at exonerative scenarios. This is important because ITA is prone to false positives, owing to the reality most people in an organization are not threats (Cappelli et al., 2013). Table 41 presents time and accuracy results according to scenario outcome.

Table 41. Cross Tabulation—Time and Accuracy per Outcome.

		Ignorance	
Teamwork	Specialized	High	Low
		Time Implicate: 935s Exonerate: 803s Accuracy Implicate: 83% Exonerate: 66%	Time Implicate: 1422s Exonerate: 1291s Accuracy Implicate: 100% Exonerate: 83%
	None	Time Implicate: 556s Exonerate: 425s Accuracy Implicate: 66% Exonerate: 33%	Time Implicate: 1043s Exonerate: 912s Accuracy Implicate: 83% Exonerate: 50%

The experimental evidence supports Hypothesis 2, because participants under conditions of a low level of ignorance required more time to perform ITA than those under a high level of ignorance ($F(1,46)=32.037$, $p=.000$, $R^2_{adj}=.398$; $U = 60$, $p = .001$, $r = .679$). Hypothesis 1 was not supported. There was no accuracy boost to match the cost in time. Recall that there was no statistically significant difference in accuracy under either condition of ignorance and no statistically significant difference in analyst confidence between either condition of ignorance. Harold Kelly's (1973) concept of schema best explains the results: namely, participants organized in a specialized team had more than one perspective included in the information-integration process. The additional perspectives and experience afforded filled in the blanks of missing information and reduced the influence of confirmation bias. This conclusion is most evident in the

exonerative scenarios, whereby individually organized analysis resulted in the lowest accuracy.

Overall, the results indicate that insider threat analysts organized individually with access to all information are the best fit for analyst programs charged with processing a large quantity of information quickly. Similarly, the results indicate that insider threat analysts organized as specialized teams are the best fit for organizations chiefly concerned with achieving high accuracy, regardless of the higher time cost. Reducing information resources, or increasing ignorance, gives the best analyst time, but also results in the highest misattribution, when analysts are organized individually. Furthermore, there is an interaction between teamwork and ignorance whereby teamwork increases the perception of information overload under conditions of high ignorance, but reduces the perception of information overload under conditions of low ignorance. Table 42 lists the supporting research questions, analysis methods, and results.

Table 42. Supporting Research Questions, Analysis Method, and Results.

Main Research Questions		Variables	Analysis	Assessment (Statistic, Significance, Effect)
1	Do teamwork and ignorance interactively affect analyst performance?	INDEP: Team(0/1); Ign(0/1) DEP: performance(ratio)	ANOVA	No ($F(1,44)=.038, p=.847$)
2	Does teamwork affect analyst performance?	INDEP: Team(0/1) DEP: performance(ratio)	ANOVA Regression Mann Whitney U	No ($F(1,44)=.213, p=.647$) No ($t=.469, p=.640$) No ($U=265, p=.635$)
3	Does ignorance affect analyst performance?	INDEP: Ign(0/1) DEP: performance(ratio)	ANOVA Regression Mann Whitney U	No ($F(1,44)=.298, p=.588$) No ($t=.556, p=.583$) Marginally ($U= 208, p=.099, r=.238$)
4	Do teamwork and ignorance interactively affect analyst time?	INDEP: Team(0/1); Ign(0/1) DEP: Time(# seconds)	ANOVA	No ($F(1,44)=.648, p=.425$)
5	Does teamwork affect analyst time?	INDEP: Team(0/1) DEP: Time(# seconds)	ANOVA Regression Mann Whitney U	Significantly ($F(1,46)=15.198, p=.000, R^2_{adj}=.232$) Significantly ($t=3.898, p=.000, R^2_{adj}=.232$) Significantly ($U=120, p=.000, r=.499$)
6	Does ignorance affect analyst time?	INDEP: Ign(0/1) DEP: Time (# seconds)	ANOVA Regression	Significantly ($F(1,46)=32.037, p=.000, R^2_{adj}=.398$)

			Mann Whitney U	Significantly ($t=-5.660, p=.000, R^2_{adj}=.398$) Significantly ($U=60, p=.000, r=.678$)
7	Do teamwork and ignorance interactively affect analyst accuracy?	INDEP: Team(0/1); Ign(0/1) DEP: Accuracy(0/1)	ANOVA	No ($F(1,44)=.000, p=1$)
8	Does teamwork affect analyst accuracy?	INDEP: Team(0/1) DEP: Accuracy(0/1)	Logit Regression Chi-square test	Marginally ($Z=1.853, p=.063, r=.267$) Marginally ($X^2=3.630, p=.057, \phi=.275$)
9	Does ignorance affect analyst accuracy?	INDEP: Ign(0/1) DEP: Accuracy (0/1)	Logit Regression Chi-square test	No ($Z=1.853, p=.209$) No ($X^2=3.63, p=.204$)
10	Do teamwork and ignorance interact with analyst confidence?	INDEP: Team(0/1); Ign(0/1) DEP: Confidence(1–9)	ANOVA	No ($F(1,44)=.1467, p=.232$)
11	Does teamwork affect analyst confidence?	INDEP: Team(0/1) DEP: Confidence(1–9)	ANOVA Regression Mann Whitney U	No ($F(1,46)=.523, p=.473$) No ($t=-.723, p=.473$) No ($U=253, p=.456$)
12	Does ignorance affect analyst confidence?	INDEP: Ign(0/1) DEP: Confidence(1–9)	ANOVA Regression Mann Whitney U	No ($F(1,46)=.939, p=.338$) No ($t=-.968, p=.337$) No ($U=247.5, p=.388$)
13	Do teamwork and ignorance interactively affect perceptions of information overload?	INDEP: Team(0/1); Ign(0/1) DEP: InfoOvld(1-9)	ANOVA Nonparametric bootstrap simulation	Marginally ($F(1,44)=3.541, p=.067, R^2_{adj}=.040$) Marginally ($F(1,444)=30.752, p=.000, R^2_{adj}=.076$)

14	Does teamwork affect perceptions of information overload?	INDEP: Team(0/1) DEP: InfoOvld(1-9)	Regression Mann Whitney U	No ($t=-.365, p=.716$) No ($U=284.5, p=.938$)
15	Does ignorance affect perceptions of information overload?	INDEP: Ign(0/1) DEP: InfoOvld(1-9)	Regression Mann Whitney U	No ($t=-1.108, p=.273$) No ($U=251, p=.413$)
16	Does ignorance affect perceptions of social impact?	INDEP: Ign(0/1) DEP: InfoOvld(1-9)	ANOVA Mann Whitney U	No ($F(1,22)=2.588, p=.122$) No ($U=52, p=.210$)
Fixed effects questions:		Variables	Analysis	Assessment (Statistic, Significance, Effect)
17	Does any scenario affect analyst time?	INDEP: Scenario(1–4) DEP: Time (# seconds)	ANOVA Regression Kruskal-Wallis	No ($F(3,44)=1.26, p=.300$) Marginally ($t=1.912, p=.062, R^2_{adj}=.053$) No ($X^2=2.342, p=.505$)
18	Does scenario outcome affect analyst time?	INDEP: Outcome(0/1) DEP: Time (# seconds)	ANOVA Regression Mann Whitney U	No ($F(1,46)=1.415, p=.240$) No ($t=1.189, p=.240$) No ($U=248, p=.409$)
19	Does any scenario affect analyst performance?	INDEP: Scenario(1–4) DEP: performance(ratio)	ANOVA Regression Kruskal-Wallis	Marginally ($F(3,44)=2.747, p=.054, R^2_{adj}=.100$) No ($t=-1.054, p=.297$) Marginally ($X^2=6.975, p=.073, \phi=.381$)
20	Does scenario outcome affect analyst performance?	INDEP: Outcome(0/1) DEP: performance(ratio)	ANOVA Regression Mann Whitney U	No ($F(1,46)=1.998, p=.164$) No ($t=1.413, p=.164$) No ($U=221, p=.167$)

21	Does any scenario affect analyst accuracy?	INDEP: Scenario(1–4) DEP: accuracy(0/1)	Logit Regression Chi-square test	No ($Z=-.277, p=.781$) Marginally ($X^2=6.857, p=.077, \phi=.377$)
22	Does scenario outcome affect analyst accuracy?	INDEP: Outcome(0/1) DEP: accuracy(0/1)	Logit Regression Chi-square test	Marginally ($Z=1.853, p=.063, r=.267$) Marginally ($X^2=3.63, p=.057, \phi=.275$)
23	Does any scenario affect analyst decision confidence?	INDEP: Scenario(1–4) DEP: confidence(1–9)	ANOVA Regression Kruskal-Wallis	Significantly ($F(3,44)=5.775, p=.002, R^2_{adj}=.234$) No ($t=1.655, p=.104$) Significantly ($X^2=12.123, p=.007, \phi=.502$)
24	Does scenario outcome affect analyst decision confidence?	INDEP: Outcome(0/1) DEP: confidence(1–9)	ANOVA Regression Mann Whitney U	Significantly ($F(1,46)=18, p=.000, R^2_{adj}=.266$) Significantly ($t=4.242, p=.000, R^2_{adj}=.266$) Significantly ($U=125, p=.001, r=.499$)
25	Does any scenario affect perceptions of information overload?	INDEP: Scenario(1–4) DEP: InfoOvld(1-9)	ANOVA Regression Kruskal-Wallis	No ($F(3,44)=.362, p=.781$) No ($t=.272, p=.786$) No ($X^2=1.412, p=.703$)
26	Does scenario outcome affect perceptions of information overload?	INDEP: Outcome(0/1) DEP: InfoOvld(1-9)	ANOVA Regression Mann Whitney U	No ($F(1,46)=.373, p=.545$) No ($t=-.610, p=.544$) No ($U=257.5, p=.499$)
Blocking variable questions:				
27	Does age affect analyst time?	INDEP: Age(#years) DEP: Time(# seconds)	Regression	No ($t=.224, p=.823$)
28	Does gender affect	INDEP: Gender(0/1)	Regression	No ($t=1.162, p=.251$)

	analyst time?	DEP: Time(# seconds)		
29	Does education affect analyst time?	INDEP: Education(1–4) DEP: Time(# seconds)	Regression	No ($t=-.910, p=.367$)
30	Does experience affect analyst time?	INDEP: Experience(#years) DEP: Time(# seconds)	Regression	No ($t=-.119, p=.905$)
31	Does age affect analyst accuracy?	INDEP: Age(#years) DEP: Accuracy(0/1)	Logistic regression	No ($Z=-1.554, p=.120$)
32	Does gender affect analyst accuracy?	INDEP: Gender(0/1) DEP: Accuracy(0/1)	Logistic regression	No ($Z=1.580, p=.114$)
33	Does education affect analyst accuracy?	INDEP: Education(1–4) DEP: Accuracy(0/1)	Logistic regression	No ($Z=1.522, p=.127$)
34	Does experience affect analyst accuracy?	INDEP: Experience(#years) DEP: Accuracy(0/1)	Logistic regression	No ($Z=-.355, p=.722$)
35	Does age affect analyst performance?	INDEP: Age(#years) DEP: Performance(ratio)	Regression	No ($t=-1.67, p=.102$)
36	Does gender affect analyst performance?	INDEP: Gender(0/1) DEP: Performance(ratio)	Regression	No ($t=1.287, p=.204$)

37	Does education affect analyst performance?	INDEP: Education(1–4) DEP: Performance(ratio)	Regression	No ($t=1.101, p=.276$)
38	Does experience affect analyst performance?	INDEP: Experience(#years) DEP: Performance(ratio)	Regression	No ($t=-.418, p=.677$)
39	Does age affect analyst confidence?	INDEP: Age(# years) DEP: Confidence(1–9)	Regression	No ($t=-.929, p=.357$)
40	Does gender affect analyst confidence?	INDEP: Gender(0/1) DEP: Confidence(1–9)	Regression	No ($t=.036, p=.971$)
41	Does education affect analyst confidence?	INDEP: Education(1–4) DEP: Confidence(1–9)	Regression Kruskal-Wallis	Marginally ($t=2.32, p=.024, R^2_{adj}=.085$) No ($X^2=5.456, p=.141$)
42	Does experience affect analyst confidence?	INDEP: Experience(#years) DEP: Confidence(1–9)	Regression	No ($t=1.049, p=.300$)
43	Does age affect the perception of information overload?	INDEP: Age(#years) DEP: InfoOvld(1-9)	Regression	No ($t=.107, p=.915$)
44	Does gender affect the perception of information overload?	INDEP: Gender(0/1) DEP: InfoOvld(1-9)	Regression	No ($t=.985, p=.329$)
45	Does education affect	INDEP: Education(1–4)	Regression	No ($t=-1.293, p=.202$)

	the perception of information overload?	DEP: InfoOvld(1-9)		
46	Does experience affect the perception of information overload?	INDEP: Experience(#years) DEP: InfoOvld(1-9)	Regression	No ($t=.708, p=.482$)
47	Does age affect the perception of social impact?	INDEP: Age(#years) DEP: SocImpact(1-9)	Regression	No ($t=-5432, p=.593$)
48	Does gender affect the perception of social impact?	INDEP: Gender(0/1) DEP: SocImpact(1-9)	Regression	No ($t=.649, p=.523$)
49	Does education affect the perception of social impact?	INDEP: Education(1–4) DEP: SocImpact(1-9)	Regression	No ($t=-.136, p=.893$)
50	Does experience affect the perception of social impact?	INDEP: Experience(#years) DEP: SocImpact(1-9)	Regression	No ($t=-1.079, p=.293$)

VI. CONCLUSION

This chapter presents a summary of the dissertation. The summary includes the theoretical concepts that emerged from a literature review, a review of the constructs derived from the theoretical concepts, an overview of the experimental apparatus, and a synopsis of the experimental results. Theoretical contributions, recommendations, limitations, and suggestions for future work follow the experimental results. The chapter concludes with a restatement of each hypothesis, the statistical tests used for analysis, and the results of each hypothesis test.

This research tested theories of attribution and process loss as they pertain to ITA performance. The lack of theory available explaining ITA performance engenders a perception that ITA is more an art form rather than a science (Utin, 2008, p. 168; Sellen, 2016; Wittcop, 2017). This dissertation fills a part of that gap by controlling factors fundamental to ITA and quantitatively assessing the effects of variation in those factors. The ITA factors emerged from interviews, insider threat conferences, formal insider threat analysis training, and a detailed literature review. The literature review indicated that information overload is a problem for ITA analysts (Cappelli et al., 2012, p. 196; Garst & Gross, 1997). I interpreted this to mean that information overload reduces analyst accuracy and promptitude. This work offers two ways to overcome information overload: reduce information in the form of ignorance, and distribute information between more people in the form of teamwork. Ignorance and teamwork, in the light of attribution theory and process loss theory, are the main factors explored throughout this dissertation.

This dissertation answers the question “is insider threat analyst performance controllable?” Theories of information overload and underload imply that suboptimal conditions, such as too little or too much information, will detrimentally affect people who perform ITA. New technology produced a large corpus of software applications that both reduce information overload and increase information usefulness, but the technologies are only as useful as the human analyst can benefit from their employment. This research is focused on the human analyst rather than any specific technology

because ITA remains a human intensive task (Goldberg, Young, Memory, & Senator, 2016; Cappelli et al., 2012, p. 14).

Due to the human intensive nature of ITA, organizations resort to increasing both the information references and number of people required to accommodate the demand for effective insider threat organizational programs (CNSS directive 504, NITTF-2014-008, SPAWAR). This research does not dispute that more people and information references will result in better ITA, rather this research seeks to provide evidence that there are conditions under which people and information resources can provide more optimal ITA depending on informational and temporal constraints.

Drawing heavily from Sweller's (1988) theory of cognitive load and Galbraith's (1977) contingency theory of organizations, I identified two ways to reduce information overload: reduce the information load and organize people to better accommodate the load. The lack of information was quantified as ignorance based on Denby and Gammack's (1999) taxonomy. The experimental apparatus employed ITA references derived from Guido and Brooks (2013) and Brackney and Anderson (2004) and partitioned the references according to Kelley's (1973) covariation model. This research focused on the individual level of analysis to better understand how various conditions of ignorance and teamwork affect individual ITA performance in terms of time and accuracy. In order to maintain an individual level of analysis between experimental groups, I organized groups into horizontally specialized teams following Daft (2007). The structure allowed only one person to perform ITA under any experimental condition and additional people in a team configuration processed available references to inform the analyst performing ITA.

This research is important because ITA is a relatively new concept in the cybersecurity sector and in order to be effective, it is important to explore its strengths and weaknesses. Programmatic sensor information is generally stripped of context by virtue of its nature (Wang, 2013). Computers seek a pattern match in data symbols regardless of meaning and people must assign meaning to the data and integrate it with other forms of threat intelligence in order to perform effective ITA. This research is a rare test of ITA that uses externally valid top secret cleared GS-12 equivalent participants

who have all received insider threat training and were fully cognizant of the conduct expected of those who hold the same clearance. How the participants performed ITA under various conditions lends insight to how ITA programs are best organized under various informational and temporal constraints. This research uses laboratory experimentation to determine how varying conditions of ignorance and teamwork affect analyst performance in terms of time, accuracy, and confidence.

A. METHOD

This dissertation utilized a 2 x 2 factorial research design and experimental stimuli in a laboratory setting to empirically test externally valid participants. Participants were selected according to SPAWAR recommendations and experimental stimulus consisted of four scenarios (Appendix B) adapted from the National Insider Threat Task Force (NITTF) Insider Threat Analyst Training Course. Participants were incentivized with a Silver Eagle silver bullion coin for a correct ITA according to the NITTF scenario script. The four scenarios were organized within an online role based access controlled (RBAC) knowledge sharing environment (KSE) experimental apparatus. The apparatus KSE software is suitable due to its employment in several federal insider threat programs. Participants interfaced with the apparatus using PC laptops and Microsoft's Internet Explorer web browser to review scenario details and determine whether an insider was a threat or not according to the federal adjudicative guidelines for access to classified information.

The research design measured performance in terms of time and accuracy. Analogous with triple constraint theory (Goldratt & Cox, 2016), the results indicate that speed and accuracy are exclusive under various conditions of ignorance and teamwork. Ancillary to time and accuracy, the apparatus survey module recorded the subject's perception of information overload and confidence in their ITA decision. The research addressed the perception of social impact to capture any social loafing effect (Latane et al., 1979) and accounted for demographic blocks that could contribute to variability in the dependent measures. The experimental apparatus measured the ancillary constructs with Likert type survey items adapted from pre-validated research.

The experiment leveraged a web server to record analysis time and response data to an Excel spread sheet. The Excel data was imported into SPSS/Risk Simulator and tested eight hypotheses with regression analysis, a 2 x 2 ANOVA, bootstrap simulation, and non-parametric statistical analyses. Non-parametric tests were necessary to augment parametric tests due to the small sample size and categorical data.

B. CONTRIBUTION

This research contributes to the academic process of transitioning ITA from an art form to a science. This work does so by controlling ITA conditions within an explicitly documented laboratory experimental apparatus capable of scientifically replicable ITA performance effects. The results from this research show that ITA performance is predictable under various conditions of ignorance and teamwork. This new knowledge informs a contingency view of organizing analysts under various informational and temporal constraints.

The theoretical contributions of this research include a test of process loss theory applied to the insider threat to cybersecurity. Cybersecurity theories exclusive of insider threats are well established, but the lack of theory for ITA is a clear gap in knowledge that this research attempted to bridge. This research juxtaposed conditions between two prevailing ITA teamwork conditions under two conditions of ignorance. Ignorance is a factor of specific interest because insider threat analysts need to make inferences under various conditions of ignorance by the nature of the job. The two ITA test case teamwork conditions are replications of two agencies identified in Kelly and Anderson's (2014) descriptions of ITA organizations. This research operationalized the contingent ITA structures as horizontally specialized team and individual ITA. This research is the first quantitative assessment of ITA structural contingency and stands alone as an empirical test of ITA at the time of this writing.

C. FINDINGS

This research identified: a) how ignorance affects ITA time, b) how teamwork affects ITA accuracy, c) how teamwork affects ITA time, d) how teamwork and ignorance interact to affect perceptions of information overload, and e) how scenario

outcome affects ITA accuracy. Low ignorance compelled more information processing and consequently caused increased ITA time. The more interesting results of this dissertation are how teamwork affected time and accuracy under each condition of ignorance.

The experimental data revealed that teamwork is more sensitive to the information overload conditions inherent to time constrained ITA. The median time that insider threat analysts took to perform ITA was considerably greater when organized in a team over those organized as individual. Roughly analogous to “the mythical man month” (Brooks, 1995), this finding strongly suggests that efforts to increase ITA promptitude by introducing teamwork will have the opposite effect. The finding was consistent under both high and low ignorance conditions reflected in the experiment results whereby team analysts consumed 60% and 51% greater ITA time, respectively.

Pertinent to these findings I conclude that the increase in ITA time comes with an increase in accuracy under low ignorance conditions. The experimental data revealed that when information was split between a team of specialists who informed an analyst, the analyst’s accuracy increased by 37% over analysts who individually assessed the same information under low ignorance conditions. The experimental results suggest that given low ignorance, a reasonable ITA analyst should demonstrate near perfect accuracy. The lower perception of information overload for specialized teams under low ignorance conditions than individual ITA under the same low ignorance condition implied a lower “information pruning” (Savolainen, 2007) effect. It follows that since information pruning was less likely to occur, information extraction from the data (Meadow & Yuan, 1997, p. 701) was better for specialized teams than with individuals under the same low ignorance conditions.

The findings strongly suggest that the perception of information overload has effects independent of time constraints. Teamwork conditions interacted with ignorance conditions to cause various perceptions of information overload. The perception of information overload decreased by 30% when information references were split between specialists under low ignorance conditions. In contrast, the perception of information overload increased by 30% when information references were split between specialists

under high ignorance conditions. This finding reveals that in the absence of a time constraint, teamwork can cause variable perceptions of information overload depending on available information. This finding is consistent with Staats's (2012) experiment that revealed teamwork interacts with task complexity.

An unexpected finding that was not a part of the research question is how expected scenario outcome affected accuracy. Analysts are good at implicating a genuine insider threat as they correctly identified an insider threat in 83.3% of trials. However, analysts were only slightly better than chance at exoneration scenarios, as they incorrectly implicated an innocent individual in 41.7% of trials. This is perhaps the most interesting finding in this research because the participants were all TS-cleared, graduate level educated, who had all completed insider threat training and used the adjudicative guidelines to inform their ITA. Furthermore, individual analysts were no better than chance when evaluating only exoneration scenarios under either high and low ignorance conditions, 33% and 50% accuracy, respectively.

In summary, experimentation results supported four out of eight hypotheses in this dissertation. The experiments demonstrated that analysts organized in horizontally specialized teams, under the same ignorance level, will be more accurate than those organized individually. Furthermore, experimentation demonstrated that teamwork can increase accuracy at the cost of time. I apply theories of attribution and process loss to explain the phenomenon.

1. Attribution Theory Explanation

Insider threat analysis proceeded from anomalous behavior presented as stimulus. People operate as naïve psychologists who search for a cause to attribute to anomalous behaviors (Heider, 1958). The cognitive process in which people make attributions is based on consensus, consistency, and distinctiveness (Kelley, 1973). Consensus is how much a behavior is in common with the societal norm and consistency/distinctiveness are person-within characteristics (Harvey, et al., 2014). According to Harvey, et al., low consensus behavior engenders internal attributions unless otherwise mitigated by high consistency and high distinctiveness. Similarly, from the perspective of ITA, an

anomalous behavior from societal norms may not be truly anomalous from the person-within perspective. Rather, anomalous behavior, due to some mitigating personal circumstance, may be expected due to some external mitigating circumstance. This research revealed that when information was not available that could inform the within-person perspective, analysts were more likely to draw on personal experience to infer consistency/distinctiveness options from which they form causal attributions. This is evident because teams were more accurate than individuals when under the same ignorance level.

This experiment revealed that multiple analysts, with the all available references split exclusively between them, were more accurate than one person with all available references. This is best explained by schemata in attribution theory (Kelly & Michela, 1980). Causal attribution is the subjective conceptualization of how multiple causes must combine to produce a certain effect. Schemata inform an assignment of multiple causes for specific events. Multiple people offer additional perspectives over individuals because schemata are informed by past experience. Group decision making is known to be better than that of an individual (Brodbeck, et al., 2007) but this experiment only allowed one individual, the analyst, all the information to perform an analysis. There was no group decision making yet accuracy increased with teamwork. It follows that the additional perspectives of the specialists on his team informed the analysts' schemata. The enhanced schemata informed additional options to form causal attributions that ultimately resulted in higher accuracy.

2. Process Loss Theory Explanation

The increase in accuracy came at a significant cost of time. This result was unexpected because classic specialization theory posits that assigning parts to specialists “almost certainly speed[s] up the solution process” (March & Simon, 1958, p. 181). Thompson (1967) detailed types of interdependence that specialization compels in organization theory and Steiner (1972) described the effects of interdependence in Process Loss Theory. According to these theories, interdependent tasks are prone to process loss. The experiment organized analysts into Steiner's complimentary model,

where no individual team member acting alone had the necessary resources to complete the ITA task. According to Process Loss Theory, process loss can occur any time someone on a team finishes a subtask before another in a complimentary model. This theory posits that whatever time was saved by distributing the work between specialists was less than the time used reintegrating the information for a single insider threat analyst. The time lost in reintegration is explained by the coordination overhead that emerges when interdependence increases (Katz-Navon, 2005).

D. SUMMARY

This dissertation provided evidence that ITA is controllable by varying conditions of teamwork and ignorance to produce measurable and independent performance effects. The research design identified ITA accuracy and ITA time as performance constructs and identified ITA confidence, perception of information overload, and perception of social impact as ancillary constructs. The research presented an apparatus to measure the constructs within a laboratory controlled experiment. The experiment varied the amount of information, or ignorance level, under two conditions of teamwork. The research produced eight testable hypotheses that were quantitatively assessed with both parametric and non-parametric statistical tests including a bootstrap simulation technique. Table 43 presents the results of the hypothesis testing.

Table 43. Hypothesis Test Results.

Hypothesis	Analysis Method	Statistic, Significance, Effect	Assessment
1. A higher level of ignorance will cause lower ITA accuracy.	Logistic regression Chi-square test	$Z=1.853, p=.104$ $X^2=3.63, p=.102$	Not supported. Ignorance did not cause lower accuracy likely due to experimentally fixed effect in implication scenarios indicated by Q21 – 24 results.
2. A lower level of ignorance will cause higher ITA time.	ANOVA Regression Mann-Whitney U	$F(1,46)=32.037, p=.000, R^2_{adj}=.398$ $t=-5.660, p=.000, R^2_{adj}=.398$ $U=60, p=.000, r=.678$	Supported. Decreasing ignorance caused a corresponding increase in analysis time. Ignorance level variations explained 40% of the variability in analysis time.
3. A higher level of ignorance will cause lower ITA confidence.	ANOVA Regression Mann-Whitney U	$F(1,46)=.939, p=.169$ $t=-.968, p=.168$ $U=247.5, p=.194$	Not supported. Analysts were not less confident in their assessments when ignorance level was increased.
4. Teamwork will cause higher	Logistic	$Z=1.853, p=.063, r=.267$	Supported. Horizontally specialized teamwork marginally increased ITA

Hypothesis	Analysis Method	Statistic, Significance, Effect	Assessment
ITA accuracy.	regression Chi-square test	$X^2=3.630, p=.057, \phi=.275$	accuracy indicated by a marginal statistical significance and moderate effect size.
5. Teamwork will cause higher ITA time than individual work.	ANOVA Regression Mann-Whitney U	$F(1,46)=15.198, p=.000, R^2_{adj}=.232$ $t=3.898, p=.000, R^2_{adj}=.232$ $U=120, p=.000, r=.499$	Supported. Horizontally specialized teamwork caused analysts to take significantly more time to perform ITA. Teamwork explained 23% of the variability in ITA time.
6. Teamwork will cause higher ITA confidence than individual work.	ANOVA Regression Mann-Whitney U	$F(1,46)=.523, p=.236$ $t=-.723, p=.236$ $U=253, p=.228$	Not supported. Organizing participants in a horizontally specialized team did not increase ITA confidence over those organized as individuals.

Hypothesis	Analysis Method	Statistic, Significance, Effect	Assessment
7. Teamwork and ignorance will interact with perceptions of information overload.	ANOVA Bootstrap Simulation	$F(1,44)=3.541, p=.067, R^2_{adj}=.040$ $F(1,444)=30.752, p=.000, R^2_{adj}=.076$	Supported. Teamwork and ignorance marginally interacted with perceptions of information overload. Teamwork decreased information overload under low ignorance conditions, but increased overload perceptions under high ignorance conditions.
8. A lower level of ignorance will cause higher perceptions of social impact.	ANOVA Mann-Whitney U	$F(1,22)=2.588, p=.061, R^2_{adj}=.065$ $U=52, p=.105, r=.180$	Not supported. Reducing ignorance did not increase perceptions of social impact.

E. RECOMMENDATIONS

The results show that introducing teamwork in the form of horizontal specialization may increase accuracy; however, the increase in accuracy comes at the cost of time. Teamwork is not an effective method of increasing the promptitude of ITA because the experimental results revealed a negative relationship between teamwork and analysis time even though no group decision making existed in the experiment. The implication is that individuals are better suited than teams for performing ITA under temporal constraints, but specialized teams are better when there are no temporal constraints.

1. Enhance “Mitigating Factors” in the Federal Adjudicative Guidelines for Access to Classified Information

A theoretical understanding of ITA is critical to protect organizational assets from hackers, cowards, and thieves. Threat assessment is not useful to assist with identifying a harmful person after a crime; rather it should be a method for identifying those with the propensity to harm before it happens. Continuous evaluation is a step in the right direction but is, by its nature, reactive. The other end of insider threat continuum is implicating innocent people as insider threats. The results of this experiment strongly suggest that current insider threat training is good at informing insider threat indicators, but is lousy at informing the factors that mitigate insider threat indicators. The “cyber awareness challenge” and other similar insider threat training programs may cast too wide a net, resulting in an unacceptably high false positive rate analogous to “the boy who cried wolf.”

This research presented an equal number of insider threat implication and exoneration scenarios and found that analysts tend to implicate innocents even when using the “adjudicative guidelines for access to classified information” to perform insider threat assessments as are used by top intelligence agencies. According to Cappelli et al. (2012), most insiders are loyal hard working employees, and the insider threat is the exception. If this is true, false positives may have a disproportionate impact on legitimate insider threat implications. For example, assume 5 out of 100 employees are genuine

insider threats. If the findings of this experiment applied to that assumption, 42 innocents would be implicated for each genuine insider threat exonerated. Current insider threat training and adjudicative guidelines must put more focus on mitigating factors, specifically those that inform the “person-within” dimension, to supplement the current understanding of insider threat indicators. The adjudicative guidelines for access to classified information have changed very little over the past two decades and may need more specific language to be effective in the context of today’s high threat environment. Furthermore, mitigating factors should be integrated into ITA analytical tools to reduce the prevalence of false positives.

2. Apply Attribution Theory to Computational Anomaly Detection

There is a problem with how computers software seeks out insider threats. Currently, ITA software seeks out behavior patterns that indicate threatening behavior, but do not simultaneously evaluate mitigating factors. For instance, working odd after hours, but doing so after taking a four-day leave (perhaps catching up on work). This is an example of a relationship that an analyst would assess in order to mitigate an insider threat indicator.

In the case of implication scenarios, this research demonstrated that analysts who received only organizational level information defaulted to implication without verifying behaviors warranted the response. This is because the anomaly, unless otherwise explained, was intuitively a threat to cybersecurity. Likewise, analysts who received personal information could find alternative explanations for anomalous behaviors such that they would expect the actions when given personal perspective. Analysts tended to prune the information in physical and network activity logs unless they were specialized to the tedious task. Specializing people to do the work resulted in about 50% more time to perform the same analysis. Perhaps speculation, I doubt humans would stay as focused on the task over long periods of time as those in the experiment did for a short time.

Software analytics capable of covariation modeling such as this are an appropriate direction toward computationally modeling ITA to reduce false positives. Current insider threat analytics identify behavior deviations, but require substantial human cognition to

assess the deviations relative to peer groups and the person-within circumstance. The reason covariation modeling is a difficult task is because specifying relationships between anomalous behaviors is a higher level of abstraction than identifying individual anomalous behaviors. Programmatically defining a relationship is a challenge for information science because a relationship is not traditionally understood as an object of analysis.

Vector relational data modeling (VRDM) is a unique approach to implementing conceptual models. As with synapses in the human brain, VRDM gets power from connections defined as relationships. It does so with a “conceptual breakthrough by treating *relationships as objects*” (Dolk, Anderson, Busalacchi, and Tinsley, 2012, p. 1476). Data models can extend traditional cyber-security modalities to include the insider threat perspective within a covariance model. VRDM models consist of data relationships that are, by definition, configurable, extensible, and reconfigurable and yet require no computer code programming (Anderson et al., 2014).

The VRDM interoperability implication is a worthy recommendation to mention, but configurable semantic relationship mapping is more a means than an end. Semantic relationship mapping allows computer decision-making to be informed by relevant data rather than programmatically rigid computer code (Kelly, 2014; Baugess, et al., 2014; Kelly & Anderson, 2016). VRDM executable data models demonstrated the computational capacity to update the contextual relevance of data in a recursive manner by continuously updating threat models with new behavior relationships (Seng, 2016).

3. Implement Horizontal Specialization in ITA Structure

This research scientifically assessed two competing organizational structures for ITA: horizontally specialized team and individual. Horizontally specialized teams leveraged participants that focused on specific references to inform a single insider threat analyst. This structure allowed the analyst to spend cognitive resources performing ITA over making sense of the data used for ITA.

Analysts organized individually viewed the same information as those in teams, but performed worse ITA in terms of accuracy, yet decisively better ITA in terms of time.

Recall that the two structures were similar at implicating the insider threat, but specialized teams were better at warranted exonerations. This implies that finding the insider threat is not as big a problem as filtering out the noise of false positives. Shannon's theory of information provides that signal must overcome noise to be useful. I suggest that reducing the noise of false positives in ITA should have priority over decreasing analysis time. Logically, any time savings from individual ITA would be lost in investigative resources necessary to subsequently adjudicate false positives.

F. LIMITATIONS

The experiment relied on an assumption that Kelley's (1973) covariation model explains how insider threat analysts reason through the ITA process. Video recorded ITA interactions between team members were consistent with the model, but individuals performed ITA silently. Individual participants were not asked to talk out their thoughts in subsequent ITA as to do so could invalidate the data. Future research should validate that individual ITA and team ITA are equally explainable by Kelley's (1973) covariation model by requesting both individual and team ITA participants talk out their thought process. This is important because the experimental apparatus partitioned ITA references between each ignorance condition according to Kelley's (1973) model.

This dissertation assessed ITA in a single inference cycle, when in reality, ITA must accommodate a continuous flow of stimulus from a multitude of ITA references. The experiment did not leverage the full range of ITA software applications because it would be cost prohibitive and the training requirements on the participants would be too burdensome for the scope of this research. Replaying genuine network traffic in real time through a set of ITA software applications, while simultaneously injecting each scenario stimulus, would increase the external validity of the experiment and is a suggestion for future work.

Participants were instructed to use the adjudicative guidelines to inform their ITA. As a result, ITA was only as good as the participants interpreted the adjudicative guidelines. Participants received training on insider threat but they received no training on how to interpret the adjudicative guidelines. Questions pertaining to interpretation of

the adjudicative guidelines did not arise until after some participants completed the experiment. No additional insight was provided to subsequent participants who requested clarification so not to invalidate the experiment. Future experimentation should provide clear interpretation of each adjudicative guideline prior ITA.

G. FUTURE WORK

According to Housel and Waldhard (1981, p. 376), “fruitful research often asks more questions than it answers.” A remaining question involves the time limit for ITA. If an additional group was added that was given a reasonable time limit to complete their task, what would be the outcome? The insider threat experiment did not include a time limit to ITA because a reasonable time limit for ITA under each test condition was unknown at the onset of the experiment. The next step would be to apply a moderate time constraint to the test groups and determine if the performance effects from this research are consistent when information overload is introduced as a factor due to time limitations.

This research identified Cressey’s (1953) fraud triangle, Kelley’s (1973) covariation model, Heuer’s (1999) analysis of competing hypotheses, and Fein and Vossekuil’s (1998) threat assessment principles as closely related crime prediction methods but did not assess the best method for ITA. This research also investigated the effects that certain conditions of teamwork and ignorance have on the general ITA method adapted from the adjudicative guidelines for determining access to classified information. I chose this ITA method because there is currently no known “best method” for ITA and federal programs generally defer to the adjudicative guidelines. As a result, a test under conditions of black box analysis was more externally valid and appropriate for this research. Future research that juxtaposes the different methods using real life scenarios may determine which method is best for predicting insider threats.

ITA reference selection may have a greater impact than either of the factors tested in this dissertation. This research used Kelley’s (1973) covariation model to partition references per either the organizational or personal perspectives that each reference informed. CNSS directive 504 requires a minimum of user activity monitoring and Guido and Brooks (2013) list several ITA references. Empirical research that assesses the

effectiveness of each ITA reference would provide valuable insight into which references can contribute to the most optimal ITA. By pruning all but the most useful ITA references, management may reduce information overload while limiting the associated negative impact on accuracy.

Future research should consider how cognitive bias affects insider threat analysis. This work considered analyst predisposition with the question “Which generally describes your predisposition to the accused: innocent until proven guilty or guilty until proven innocent?” There was no statistically significant relationship between predisposition and accuracy or time. The question itself was not validated in prior research and likely did little to capture the true world view of the analyst. Subsequent experimentation should ask participants a similar question on a multipoint scale for greater specificity that may reveal some relationship between world view and analyst accuracy.

This work reported the results of a cross sectional analysis of ITA analyst performance. Because each analyst assessed performed ITA only once, the experiment could not capture any learning effect. A repeated measures design could capture any latent learning effects and determine if a relationship with expertise exists. The expectation is that more experienced ITA analysts will demonstrate a smaller learning effect than novice ITA analysts. Repeated measures in this experiment would require either more participants or more scenarios to ensure no one sees the same scenario stimulus twice. If more scenarios are made available, future research should consider a repeated measures design.

Perceived threat level could have biased the results because the suspicion of espionage may have appeared more serious than suspicion of adultery, unreported sexual encounters with foreign nationals, or mishandling classified information. Perhaps the perceived threat level and not the guilt of the subject in Scenario 2 was the more proximate cause of no participant getting the scenario incorrect. If that is the case, the effect is due to the participant’s cognitive bias and is not experimentally fixed. Future research should ensure that insider threat scenarios are equal in perceived threat level.

This would provide evidence for or against analysts being more inclined to escalate a case when no adjudicative guidelines are violated due to being overly cautious.

In conclusion, this work tested only two factors of information overload. Future research can increase the external validity by testing additional factors that contribute to information overload; namely, information rate. Insider threat analysts must accommodate an endless flow of information from various software applications. Recent research at NPS found that analyzing large volumes of data is a challenge for ITA (Campbell, 2017). Irvine (2016) modeled information flow within an “Extend” simulation environment and demonstrated how analysts can become overloaded. Analysts will focus only on the highest perceived threat level alerts while overlooking lower perceived threats when overloaded. False positives may increase as analysts chose to err on the side of caution as this research demonstrated. Future research should include signals analysis to understand how ITA analysts best identify genuine insider threats out of the “noise” of false positives. Additional laboratory testing may verify Irvine’s (2016) Extend simulation results with laboratory experimental design using human analysts to better understand how information overload affects human ITA analysts. A better understanding of how additional factors for information overload affect ITA will empower managers to better design ITA processes to mitigate insider threats.

APPENDIX A. PERSONAL CORRESPONDENCE

Personal communications are listed below. First are emails from the NPS security office that I used to determine my sample size. Second is an email from the National Insider Threat Task Force who stated that both highly funded insider threat programs and minimally funded programs are successful, but no metrics are available to empirically test performance in a higher fidelity manner. The communication confirmed a lack of empirical studies that evaluate insider threat analysis performance, a gap in research this dissertation seeks to contribute. Figure 5 presents the student population with requisite training and clearance requirements to participate in the research. Figure 6 presents the communication from the NITTF.

Figure 5. TS-Cleared Students with Insider Threat Training at NPS.

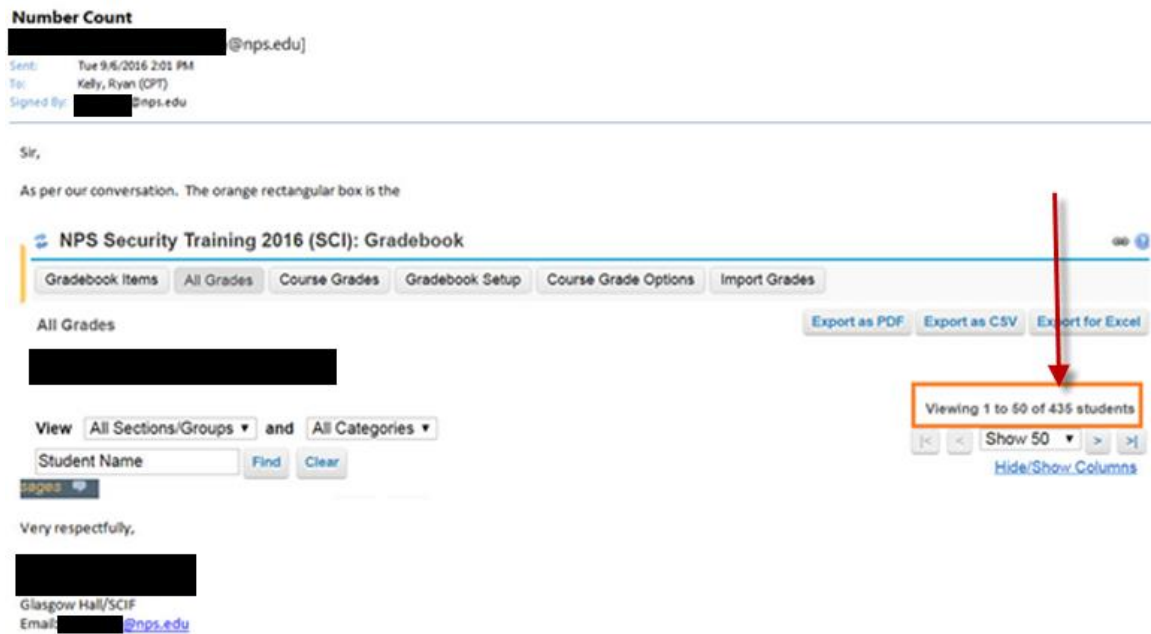


Figure 6. Personal Communication from National Insider Threat Task Force.

From: [REDACTED]
Sent: [REDACTED]
To: 'Ryan Kelly'
Subject: Follow-up

Ryan,

[REDACTED]

[REDACTED]

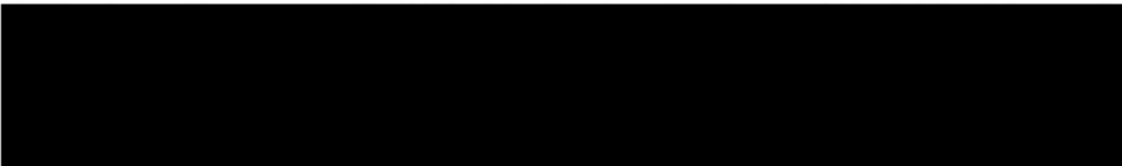
[REDACTED]

DIA as you pointed out has a solid program, but all of the IC have successful programs in place, and to some degree have benchmarked from each other, of course they have the least issue with funding and resources. I know one of the programs that Navy is looking at is the USCG (US Coast Guard).

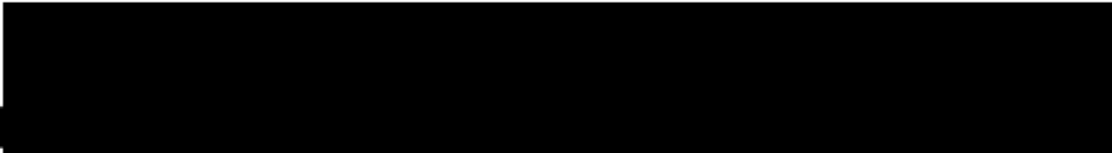
There are various tools that D/A are using and employing - I will put you in touch with the NITTF Tech team, but any discussion on that type of stuff will have to be kept on high side.

Some success has come or been evident with \$\$, but we know of small D/A with minimal \$\$ that have done and are doing very well with their programs.

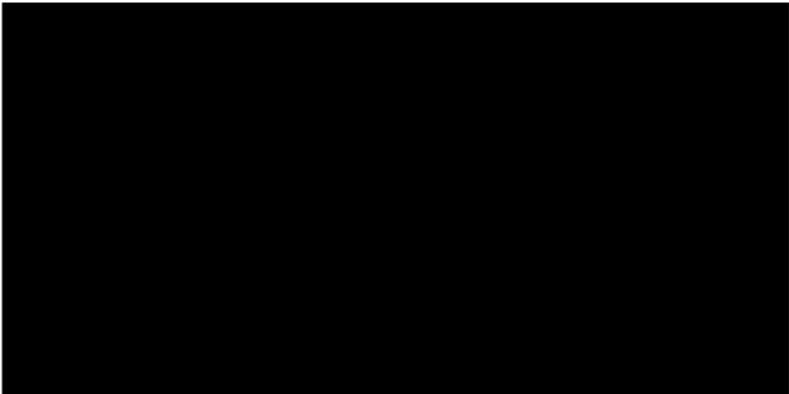
[REDACTED]



No one likes to talk much about false positive(s). But, no doubt it has been or was a concern early on as D/A began to put their programs in place. And, I have not heard of any that have been identified / associated / addressed within legal proceedings.



Don' know / am not aware of an "empirical study" done that scientifically addresses the claim...but we certainly know that no two programs are alike and based up mission the pieces and parts put in place will be different.



THIS PAGE INTENTIONALLY LEFT BLANK

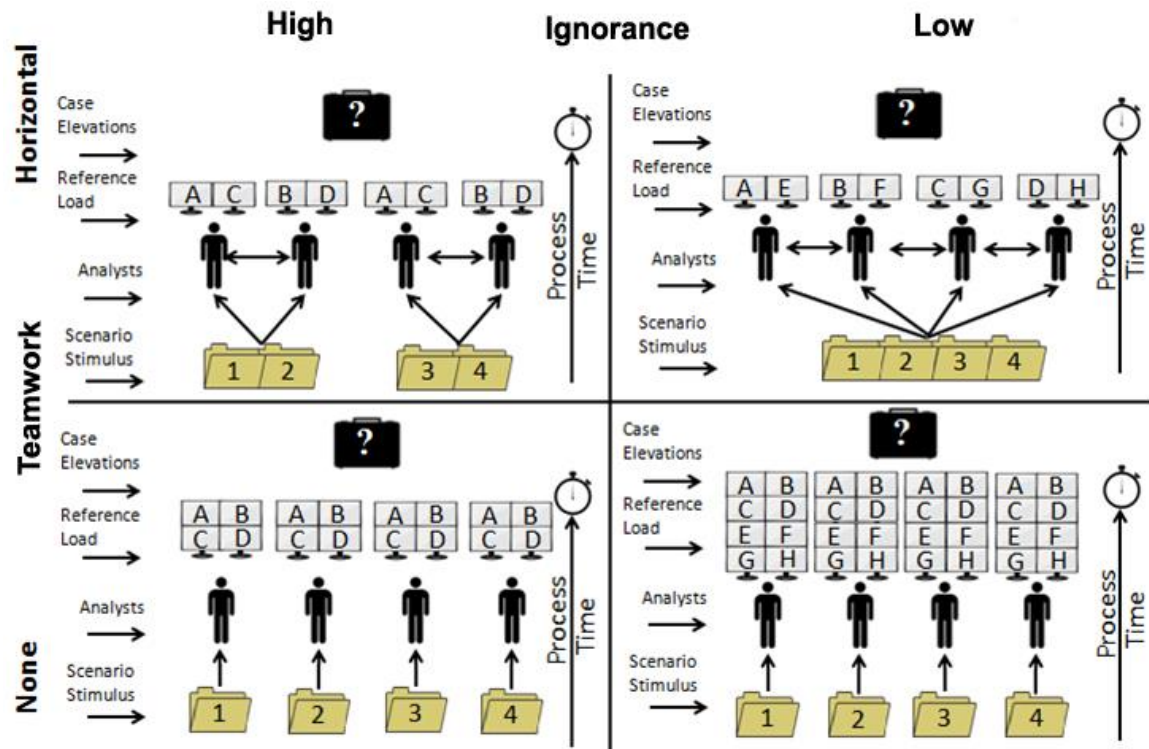
APPENDIX B. EXPERIMENT REPLICATION DOCUMENTS

This appendix provides replication documents to perform the insider threat analysis experiment with the same experimental configuration and scenarios.

A. PARTICIPANT ASSIGNMENTS

The relationship between the subjects, stimulus, and research variables are presented as an overlay within the factorial analysis in Table 44. The reference load letters correspond to the references detailed in ignorance attributes.

Table 44. Participant, Scenario, Teamwork, and Ignorance Relationships.

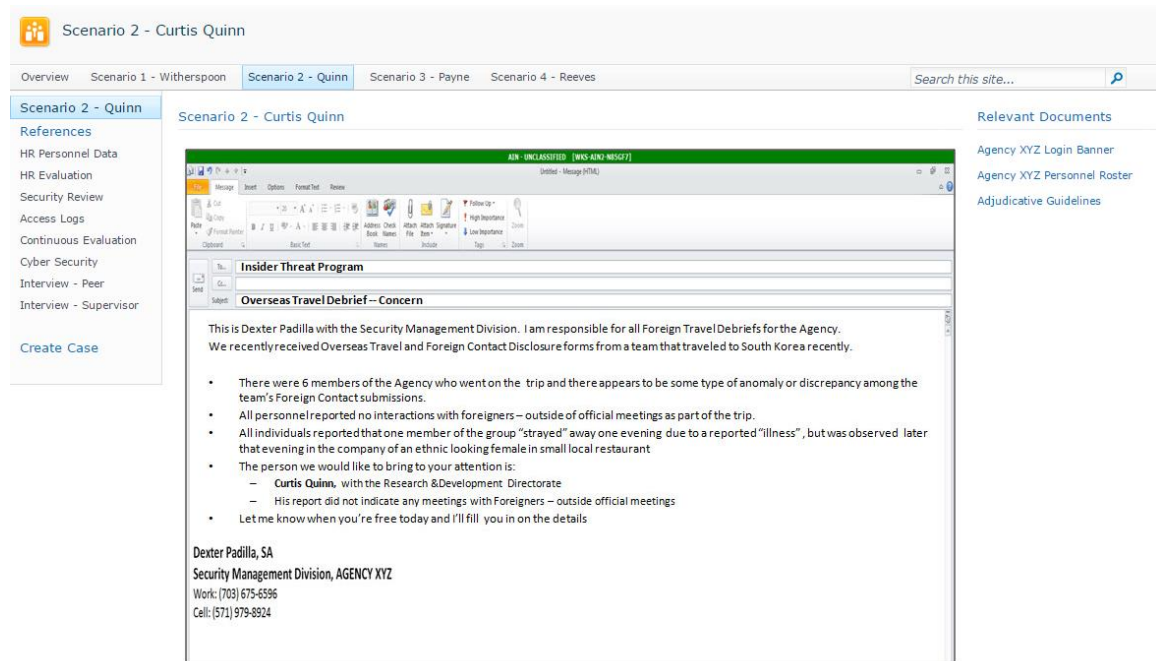


B. APPARATUS DESIGN

The experiment apparatus was constructed entirely in cyberspace. The server is located in Root 103c Distributed Information Systems Experimentation (DISE) lab. Each

participant has a unique network account. Each network account has pre-specified network permissions to view only the scenarios and references that correspond to a specified quadrant. Figure 7 presents a screenshot from the KSE with a scenario stimulus and references.

Figure 7. KSE Screenshot—Scenario Stimulus.



1. Physical Configuration

The physical apparatus configuration was straight forward. A web server, presentation monitor, research observation desk and four participant workstations were networked together in the DISE lab at NPS.

2. Server Configuration

The following scripts should be put in individual batch files to automatically create the apparatus environment. Create files with the contents of each bulleted section below and run the batch files on the SharePoint server. These groups apply participant roles to the appropriate scenario, references, and case surveys.

- Specify Reference Names—Groups.csv file contents

Scenario1
Scenario2
Scenario3
Scenario4
RefA
RefB
RefC
RefD
RefE
RefF
RefG
RefH
Case1
Case2
Case3
Case4
Professors

- Specify Participant Logins—Users.csv file contents

G1SHRHP1,Security1!
G1SHRHP2,Security1!
G1SHRHP3,Security1!
G1SHRHP4,Security1!
G1SHRLP1,Security1!
G1SHRLP2,Security1!
G1SHRLP3,Security1!
G1SHRLP4,Security1!
G1SLRHP1,Security1!
G1SLRHP2,Security1!
G1SLRHP3,Security1!
G1SLRHP4,Security1!
G1SLRLP1,Security1!
G1SLRLP2,Security1!
G1SLRLP3,Security1!
G1SLRLP4,Security1!
G2SHRHP1,Security1!
G2SHRHP2,Security1!
G2SHRHP3,Security1!
G2SHRHP4,Security1!
G2SHRLP1,Security1!
G2SHRLP2,Security1!
G2SHRLP3,Security1!
G2SHRLP4,Security1!
G2SLRHP1,Security1!
G2SLRHP2,Security1!
G2SLRHP3,Security1!

G2SLRHP4,Security1!
 G2SLRLP1,Security1!
 G2SLRLP2,Security1!
 G2SLRLP3,Security1!
 G2SLRLP4,Security1!
 G3SHRHP1,Security1!
 G3SHRHP2,Security1!
 G3SHRHP3,Security1!
 G3SHRHP4,Security1!
 G3SHRLP1,Security1!
 G3SHRLP2,Security1!
 G3SHRLP3,Security1!
 G3SHRLP4,Security1!
 G3SLRHP1,Security1!
 G3SLRHP2,Security1!
 G3SLRHP3,Security1!
 G3SLRHP4,Security1!
 G3SLRLP1,Security1!
 G3SLRLP2,Security1!
 G3SLRLP3,Security1!
 G3SLRLP4,Security1!
 Housel,Security1!
 Gallup,Security1!
 Munn,Security1!
 Boger,Security1!
 Rothstein,Security1!
 Editor,Security1!

- Add Groups - AG.bat file contents

```
FOR /f "tokens=1" %%a IN (c:\scripts\groups.csv) DO net localgroup %%a /add
```

- Add Users - AU.bat file contents

```
FOR /f "tokens=1-2 delims=" %%a IN (c:\scripts\users.csv) DO net user %%a %%b /EXPIRES:NEVER /PASSWORDCHG:NO /ADD
```

- Add users to groups—AddUsersToGroup.bat file contents

```
net localgroup professors boger housel munn gallup rothstein /add
```

```
net localgroup Scenario1 G1SHRHP1 G1SHRLP1 G1SLRHP1 G1SLRLP1 G2SHRHP1
G2SHRLP1 G2SLRHP1 G2SLRLP1 G3SHRHP1 G3SHRLP1 G3SLRHP1 G3SLRLP1
G1SHRLP2 G2SHRLP2 G3SHRLP2 G1SHRHP2 G1SHRHP3 G1SHRHP4 G2SHRHP2
G2SHRHP3 G2SHRHP4 G3SHRHP2 G3SHRHP3 G3SHRHP4 /add
```

net localgroup Scenario2 G1SHRHP2 G1SHRLP2 G1SLRHP2 G1SLRLP2 G2SHRHP2
G2SHRLP2 G2SLRHP2 G2SLRLP2 G3SHRHP2 G3SHRLP2 G3SLRHP2 G3SLRLP2
G1SHRLP1 G2SHRLP1 G3SHRLP1 G1SHRHP1 G1SHRHP3 G1SHRHP4 G2SHRHP1
G2SHRHP3 G2SHRHP4 G3SHRHP1 G3SHRHP3 G3SHRHP4 /add

net localgroup Scenario3 G1SHRHP3 G1SHRLP3 G1SLRHP3 G1SLRLP3 G2SHRHP3
G2SHRLP3 G2SLRHP3 G2SLRLP3 G3SHRHP3 G3SHRLP3 G3SLRHP3 G3SLRLP3
G1SHRLP4 G2SHRLP4 G3SHRLP4 G1SHRHP1 G1SHRHP2 G1SHRHP4 G2SHRHP1
G2SHRHP2 G2SHRHP4 G3SHRHP1 G3SHRHP2 G3SHRHP4 /add

net localgroup Scenario4 G1SHRHP4 G1SHRLP4 G1SLRHP4 G1SLRLP4 G2SHRHP4
G2SHRLP4 G2SLRHP4 G2SLRLP4 G3SHRHP4 G3SHRLP4 G3SLRHP4 G3SLRLP4
G1SHRLP3 G2SHRLP3 G3SHRLP3 G1SHRHP1 G1SHRHP2 G1SHRHP3 G2SHRHP1
G2SHRHP2 G2SHRHP3 G3SHRHP1 G3SHRHP2 G3SHRHP3 /add

net localgroup Case1 G1SHRHP1 G1SHRLP1 G1SLRHP1 G1SLRLP1 G2SHRHP1
G2SHRLP1 G2SLRHP1 G2SLRLP1 G3SHRHP1 G3SHRLP1 G3SLRHP1 G3SLRLP1
/add

net localgroup Case2 G1SHRHP2 G1SHRLP2 G1SLRHP2 G1SLRLP2 G2SHRHP2
G2SHRLP2 G2SLRHP2 G2SLRLP2 G3SHRHP2 G3SHRLP2 G3SLRHP2 G3SLRLP2
/add

net localgroup Case3 G1SHRHP3 G1SHRLP3 G1SLRHP3 G1SLRLP3 G2SHRHP3
G2SHRLP3 G2SLRHP3 G2SLRLP3 G3SHRHP3 G3SHRLP3 G3SLRHP3 G3SLRLP3
/add

net localgroup Case4 G1SHRHP4 G1SHRLP4 G1SLRHP4 G1SLRLP4 G2SHRHP4
G2SHRLP4 G2SLRHP4 G2SLRLP4 G3SHRHP4 G3SHRLP4 G3SLRHP4 G3SLRLP4
/add

net localgroup RefA G1SLRLP1 G1SLRLP2 G1SLRLP3 G1SLRLP4 G1SLRHP1
G1SLRHP2 G1SLRHP3 G1SLRHP4 G2SLRLP1 G2SLRLP2 G2SLRLP3 G2SLRLP4
G2SLRHP1 G2SLRHP2 G2SLRHP3 G2SLRHP4 G3SLRLP1 G3SLRLP2 G3SLRLP3
G3SLRLP4 G3SLRHP1 G3SLRHP2 G3SLRHP3 G3SLRHP4 G1SHRLP1 G2SHRLP1
G3SHRLP1 G1SHRLP3 G2SHRLP3 G3SHRLP3 G1SHRHP1 G2SHRHP1 G3SHRHP1
/add

net localgroup RefB G1SLRLP1 G1SLRLP2 G1SLRLP3 G1SLRLP4 G1SLRHP1
G1SLRHP2 G1SLRHP3 G1SLRHP4 G2SLRLP1 G2SLRLP2 G2SLRLP3 G2SLRLP4
G2SLRHP1 G2SLRHP2 G2SLRHP3 G2SLRHP4 G3SLRLP1 G3SLRLP2 G3SLRLP3
G3SLRLP4 G3SLRHP1 G3SLRHP2 G3SLRHP3 G3SLRHP4 G1SHRLP2 G2SHRLP2
G3SHRLP2 G1SHRLP4 G2SHRLP4 G3SHRLP4 G1SHRHP2 G2SHRHP2 G3SHRHP2
/add

```
net localgroup RefC G1SLRLP1 G1SLRLP2 G1SLRLP3 G1SLRLP4 G1SLRHP1
G1SLRHP2 G1SLRHP3 G1SLRHP4 G2SLRLP1 G2SLRLP2 G2SLRLP3 G2SLRLP4
G2SLRHP1 G2SLRHP2 G2SLRHP3 G2SLRHP4 G3SLRLP1 G3SLRLP2 G3SLRLP3
G3SLRLP4 G3SLRHP1 G3SLRHP2 G3SLRHP3 G3SLRHP4 G1SHRLP1 G2SHRLP1
G3SHRLP1 G1SHRLP3 G2SHRLP3 G3SHRLP3 G1SHRHP3 G2SHRHP3 G3SHRHP3
/add
```

```
net localgroup RefD G1SLRLP1 G1SLRLP2 G1SLRLP3 G1SLRLP4 G1SLRHP1
G1SLRHP2 G1SLRHP3 G1SLRHP4 G2SLRLP1 G2SLRLP2 G2SLRLP3 G2SLRLP4
G2SLRHP1 G2SLRHP2 G2SLRHP3 G2SLRHP4 G3SLRLP1 G3SLRLP2 G3SLRLP3
G3SLRLP4 G3SLRHP1 G3SLRHP2 G3SLRHP3 G3SLRHP4 G1SHRLP2 G2SHRLP2
G3SHRLP2 G1SHRLP4 G2SHRLP4 G3SHRLP4 G1SHRHP4 G2SHRHP4 G3SHRHP4
/add
```

```
net localgroup RefE G1SLRHP1 G1SLRHP2 G1SLRHP3 G1SLRHP4 G2SLRHP1
G2SLRHP2 G2SLRHP3 G2SLRHP4 G3SLRHP1 G3SLRHP2 G3SLRHP3 G3SLRHP4
G1SHRHP1 G2SHRHP1 G3SHRHP1 /add
```

```
net localgroup RefF G1SLRHP1 G1SLRHP2 G1SLRHP3 G1SLRHP4 G2SLRHP1
G2SLRHP2 G2SLRHP3 G2SLRHP4 G3SLRHP1 G3SLRHP2 G3SLRHP3 G3SLRHP4
G1SHRHP2 G2SHRHP2 G3SHRHP2 /add
```

```
net localgroup RefG G1SLRHP1 G1SLRHP2 G1SLRHP3 G1SLRHP4 G2SLRHP1
G2SLRHP2 G2SLRHP3 G2SLRHP4 G3SLRHP1 G3SLRHP2 G3SLRHP3 G3SLRHP4
G1SHRHP3 G2SHRHP3 G3SHRHP3 /add
```

```
net localgroup RefH G1SLRHP1 G1SLRHP2 G1SLRHP3 G1SLRHP4 G2SLRHP1
G2SLRHP2 G2SLRHP3 G2SLRHP4 G3SLRHP1 G3SLRHP2 G3SLRHP3 G3SLRHP4
G1SHRHP4 G2SHRHP4 G3SHRHP4 /add
```

3. Participant Scenario Reference Relationship Matrix

Role based access control will limit and allow access based on permissions granted in each server group specified in section 1. Server configuration should associate each participant with access to specific scenarios, specific references and specific case management access that corresponds to the matrix in Table 45.

Table 45. Participant Scenario and Reference Assignments.

Participant	Scenario	Scenario 1 Refs				Scenario 2 Refs				Scenario 3 Refs				Scenario 4 Refs				Scenario1
G1SHRLP1	1 2	A	C			B	D											RefA = HR Personnel
G1SHRLP2	1 2		B	D			A	C										RefB = Security Review
G1SHRLP3		3	4							A	C			B	D			RefC = Continuous Eval
G1SHRLP4		3	4							B	D			A	C			RefD = Peer Interview
G1SHRHP1	1 2 3 4	A		E		B		F		C		G		D		H		RefE = Supervisor Interview
G1SHRHP2	1 2 3 4		B		F		C		G		D		H		A		E	RefF = CyberSecurity
G1SHRHP3	1 2 3 4			C		G		D		H		A		E		B		RefG = Access Logs
G1SHRHP4	1 2 3 4			D		H		A		E		B		F		C		RefH = HR Evaluation
G1SLRLP1	1	A	B	C	D		A	B	C	D		A	B	C	D			
G1SLRLP2	2		A	B	C	D		A	B	C	D		A	B	C	D		
G1SLRLP3	3		A	B	C	D		A	B	C	D		A	B	C	D		
G1SLRLP4		4	A	B	C	D		A	B	C	D		A	B	C	D		
G1SLRHP1	1	A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H	
G1SLRHP2	2		A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H
G1SLRHP3	3		A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H
G1SLRHP4		4	A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H
G2SHRLP1	1 2	A	C			B	D											
G2SHRLP2	1 2		B	D			A	C										
G2SHRLP3		3	4							A	C			B	D			
G2SHRLP4		3	4							B	D			A	C			
G2SHRHP1	1 2 3 4	A		E		B		F		C		G		D		H		
G2SHRHP2	1 2 3 4		B		F		C		G		D		H		A		E	
G2SHRHP3	1 2 3 4			C		G		D		H		A		E		B		F
G2SHRHP4	1 2 3 4			D		H		A		E		B		F		C		G
G2SLRLP1	1	A	B	C	D		A	B	C	D		A	B	C	D			
G2SLRLP2	2		A	B	C	D		A	B	C	D		A	B	C	D		
G2SLRLP3	3		A	B	C	D		A	B	C	D		A	B	C	D		
G2SLRLP4		4	A	B	C	D		A	B	C	D		A	B	C	D		
G2SLRHP1	1	A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H	
G2SLRHP2	2		A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H
G2SLRHP3	3		A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H
G2SLRHP4		4	A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H
G3SHRLP1	1 2	A	C			B	D											
G3SHRLP2	1 2		B	D			A	C										
G3SHRLP3		3	4							A	C			B	D			
G3SHRLP4		3	4							B	D			A	C			
G3SHRHP1	1 2 3 4	A		E		B		F		C		G		D		H		
G3SHRHP2	1 2 3 4		B		F		C		G		D		H		A		E	
G3SHRHP3	1 2 3 4			C		G		D		H		A		E		B		F
G3SHRHP4	1 2 3 4			D		H		A		E		B		F		C		G
G3SLRLP1	1	A	B	C	D		A	B	C	D		A	B	C	D			
G3SLRLP2	2		A	B	C	D		A	B	C	D		A	B	C	D		
G3SLRLP3	3		A	B	C	D		A	B	C	D		A	B	C	D		
G3SLRLP4		4	A	B	C	D		A	B	C	D		A	B	C	D		
G3SLRHP1	1	A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H	
G3SLRHP2	2		A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H
G3SLRHP3	3		A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H
G3SLRHP4		4	A	B	C	D	E	F	G	H	A	B	C	D	E	F	G	H
*** For server access controls, users are assigned to groups that rotate instead of rotating user group memberships.																		
Scenario1				Scenario2				Scenario3				Scenario4						
RefA = HR Personnel				RefB = HR Personnel				RefC = HR Personnel				RefD = HR Personnel						
RefB = Security Review				RefC = Security Review				RefD = Security Review				RefA = Security Review						
RefC = Continuous Eval				RefD = Continuous Eval				RefA = Continuous Eval				RefB = Continuous Eval						
RefD = Peer Interview				RefA = Peer Interview				RefB = Peer Interview				RefC = Peer Interview						
RefE = Supervisor Interview				RefF = Supervisor Interview				RefG = Supervisor Interview				RefH = Supervisor Interview						
RefF = CyberSecurity				RefG = CyberSecurity				RefH = CyberSecurity				RefE = CyberSecurity						
RefG = Access Logs				RefH = Access Logs				RefE = Access Logs				RefF = Access Logs						
RefH = HR Evaluation				RefE = Evaluation				RefF = HR Evaluation				RefG = HR Evaluation						

C. INSIDER THREAT SCENARIO OUTCOMES

The correspondence from the NITTF describes four scenario outcomes. Two scenarios should be elevated and two should not. Two scenarios were similar in that they both pointed to an extramarital affair. The similarity of the outcomes threatened the internal validity of the scenario so I modified the Scenario 2(b) outcome by changing the marital status of the insider from married to single and changed the nationality of the questionable female from Malaysian to Chinese. The change was to see if insider threat analysts assess unintentional (non-malicious) insider threats differently than intentional insider threats. The outcome is consistent with guidance from the Adjudicative Guidelines and the NITTF outcome guidance. The four scenario outcomes in the experiment apparatus are supported by the NITTF correspondence. The outcomes are consistent with guidance from the adjudicative guidelines.

Ryan Kelly

From: [REDACTED]@dni.gov]
Sent: Monday, April 11, 2016 5:15 AM
To: Kelly, Ryan (CPT)
Subject: NITTF Hub Course Scenarios

Good Morning Ryan,

I apologize for the delay, but I had too many hot potatoes over the last two weeks.

This will be the first of a few emails to provide you the unclassified scenario injects you requested for your research.

Here's a summary of each and what I'm going to send you:

Scenarios 1: This scenario is about a hotline report of someone printing a large file in a SCIF on a weekend. The hub then gathers all available data to determine what response actions the agency should pursue. They find out the person of interest (Witherspoon) has a poor performance rating and is disputing his rating. He doesn't have a reason to be in on the weekend or to be in the building he printed the file. Additionally, he walked in the building with a backpack and presumably left the building and the premises with the printout in his backpack. The file is password protected so the students do not find out the contents or the classification of the file (one of the big unknowns). The book answer is that the file is a collection of his work efforts to dispute his rating. We do not confirm the classification of the file thru any injects. So, there are several potential outcomes. He may not have done anything wrong if the file was not classified. If the file was classified, he likely committed a security violation. There is no foreign nexus.

Scenario 2: This scenarios starts out the same for all three groups, but then diverges. The initial inject is a foreign travel debrief of six total travelers, but five of them report suspicious actions on the part of the sixth traveler (Quinn). Each group receives additional information that clouds the picture, but nothing definitive at first. By the third round of break-out sessions (and data gathering), each group has a different set of data upon which to make a recommendation for action.

- a. One group has clear evidence of a potential loss of information and a foreign nexus. That recommendation should be a referral to the FBI (We call an 811 Referral based on the Public Act of 1996, Section 811)
- b. The second group has a lot of smoke that points to an extramarital affair. Since he holds a high clearance, this is an IG, HR, or personnel security problem.
- c. The last group also has a lot of smoke but the "foreign" person Quinn was seen with turns out to be a US person, so no debrief report was necessary.

Here's what I am sending you in subsequent emails:

1. Each scenario has a facilitator script
2. Each scenario (and divergent outcomes) has a set of injects representing the data sources and gathering.
3. Each scenarios has pictures (for your amusement if nothing else)

Regards,

[REDACTED]

National Insider Threat Task Force
National Counterintelligence and Security Center (NCSC)

[REDACTED]

D. SURVEY INSTRUMENTS

The experiment presented each participant with an entrance survey, a case management survey, and an exit survey. The entrance survey (Figure 8) collected demographic data that informed blocking variables. The case management survey (Figure 9) collected information that informed the dependent variables accuracy and confidence. The exit survey (Figure 10) collected information that informed the dependent variables perception of information overload and perception of social impact.

Figure 8. Entrance Survey.

Entrance Survey - New Item

Next

Save and Close

Cancel

* indicates a required field

Which most generally describes your predisposition to an accused?
I am not asking how you think it should be, rather, how you are truly predisposed. *

☐ Guilty until proven innocent.

☐ Innocent until proven guilty.

Do you have any experience with threat analysis or investigations? *

☐ Insider threat analysis

☐ Investigations

☐ Both insider threat analysis and investigations

☐ No professional experience with either

How many years experience do you have? *

What is your age? *

What is your gender? *

☐ Male

☐ Female

What is the highest level of education you have completed? *

☐ High school

☐ Bachelor's degree

☐ Master's degree

☐ Doctorate degree

☐ Post-Doctorate degree

Figure 9. Case Management Survey.

Create Case - New Item

Next

Save and Close

Cancel

* indicates a required field

This records the date and time that the case creation was started on the server's time, please don't change this value! *

5/30/2016

3 PM

41

Please describe the details of the incident (i.e. Who, What, Where, Why, How?) *

Nature of Incident *

☒

☐ Specify your own value:

Select the Threat Type: *

☒

☐ Specify your own value:

Is this case warranted for escalation at this time? *

☐ No
 ☐ Yes

Confidence Perception *

	Low				Average				High
	1	2	3	4	5	6	7	8	9
I feel confident that my threat assessment is correct.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 10. Exit Survey.

Exit Survey -

Finish

Cancel

* indicates a required field

Small Group Dynamics *

	Low 1	2	3	4	Medium 5	6	7	8	High 9
I rushed through the task because I was considerate of my teammates time.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Because other group members did not try as hard as they could, I did not work as hard as I could on this project.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Information Overload *

	Low 1	2	3	4	Medium 5	6	7	8	High 9
For my scenario, I was overwhelmed by the amount of information I had to process to make a decision.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

E. SUPPLEMENTAL

Scenario stimulus and references are located in a restricted copy of this dissertation.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. INSTITUTIONAL REVIEW BOARD

Pursuant to SECNAVINST 3900.39, NPS requires Institutional Review Board (IRB) approval for human-subjects research, as employed in this research. This research leveraged monetary compensation as a performance incentive.

A. PAYMENT SCHEDULE

Payment of one American Eagle silver dollar (intrinsic value of \$20) will only be made for a correct insider threat analysis.

Individuals:

Participants will not be told if analysis is correct until after exit survey is complete.

Payment:

Incorrect analysis = Nothing

Correct analysis = American Eagle Silver Dollar (that has an intrinsic value of \$20)

Teams:

Participants will not be told if analysis is correct until after exit survey is complete.

Payment:

Incorrect analysis = Nothing

Correct analysis = American Eagle Silver Dollar (that has an intrinsic value of \$20). Only the participant assigned the case gets the incentive. All others on the team receive no incentive regardless of the analysis outcome. Each person on the team gets the opportunity to solve one case but must relay information to his team mate for the remaining scenario(s).

Grading Rubric:

Correct insider threat analysis corresponds to the following criteria:

Scenario 1: Exoneration - No foreign nexus, no verifiable threat data. Hearsay is insufficient evidence. Most likely explanation: Witherspoon is retaliating against supervisor's bad evaluation with complaints to Human Resources office that he is privately compiling.

Scenario 2: Insider Threat (Intentional) - Foreign nexus identified, two way communication suspected, subject has access to classified data, abnormal access times identified, mortgage payments delinquent & wife lost her job. Consensus among witnesses that Quinn was seen with a foreign woman in a foreign country. Most likely explanation: Quinn interacted with North Korean spy presumably to make his mortgage payments.

Applicable guidelines: A, B, E, F, L

Scenario 3: Exoneration - No foreign nexus, foreign woman inference: daughter, child of wife with Vietnamese first and maiden name. Debt is sporadically missed credit card payments (unsecured debt of unknown sum) does not indicate financial hardship. GS-12 Step 8 implies Payne is an older man. Most likely explanation: called in sick to visit with daughter who was in town.

Scenario 4: Insider Threat (Unintentional) - Foreign nexus identified with clear evidence of romantic relationship with a foreign national including unreported foreign travel. Evidence of alcohol abuse and high risk lacking judgment sexual behavior. Has access to classified data. Most likely explanation: Reeves is a young sex and alcohol addict who engaged in a sexual relationship with a foreign national.

Applicable guidelines: B, D, E, G, I, L

B. ANONYMOUS SURVEY CONSENT

Naval Postgraduate School
Consent to Participate in Research

Introduction. You are invited to participate in a research study entitled *the effects of specialization and reference load on insider threat analysis performance*. The purpose of this research is to test the relationship between specialization and reference load in terms of insider threat analysis performance. Your participation is important because an unwarranted escalation wastes investigative resources and could distract investigators from genuine insider threats. Likewise, not escalating a case that is warranted could allow a genuine insider threat to avoid detection.

Procedures.

You will be presented with a scenario provided by the National Insider Threat Task Force Insider Threat Training Course. You will use the information references provided to determine if suspicious activity warrants escalation to a formal investigation. All available information has already been collected prior to your analysis. Participation should take no longer than one hour for individuals, two hours for small groups, and four hours for large groups.

You will be asked to complete an entry survey to determine eligibility and demographic data, review a scenario, create a case, escalate the case if necessary, and complete an exit survey.

Location. The experiment will take place at NPS.

Voluntary Nature of the Study. Your participation in this study is strictly voluntary. You must hold or have held a Top Secret clearance, have at least a Bachelor's degree, and have not attended the NITTF training course to be eligible to participate. If you choose to participate you can change your mind at any time and withdraw from the study. You will not be penalized in any way

or lose any benefits to which you would otherwise be entitled if you choose not to participate in this study or to withdraw. The alternative to participating in the study is to not participate.

Potential Risks and Discomforts. There is a minimal risk of breach of confidentiality. We ask those that participate in a group to remain respectful of others by not discussing details of the experiment or other's involvement to others outside the study.

Anticipated Benefits. This assessment is beneficial for at least four reasons. First, this research assesses unbounded problem solving. Second, this experiment examines the effects of social impact on group dynamics when participants use unbounded systems thinking. Third, work will test the interactive effects on insider threat analysis performance under various conditions of specialization and reference load. Knowledge pertaining to these effects may help improve conditions for insider threat analysis so they can match insider threats. Lastly, this study will increase the understanding of the forces that govern the flow of information between machine and man.

You will receive an American Eagle silver dollar (market value of around \$20) if you correctly evaluate your scenario.

Confidentiality & Privacy Act. Any information that is obtained during this study will be kept confidential to the full extent permitted by law. All efforts, within reason, will be made to keep your personal information in your research record confidential but total confidentiality cannot be guaranteed. There will be no personally identifiable information stored on the server and your survey responses will be recorded on a computerized spread sheet. The records will be stored on a server owned by the DISE group that is located in Root 103c

Points of Contact. If you have any questions or comments about the research, or you experience an injury or have questions about any discomforts that you experience while taking part in this study please contact the Principal Investigator, Dr. Dan Boger, dboger@nps.edu. Questions about your rights as a research subject or any other concerns may be addressed to the Navy Postgraduate School IRB Chair, Dr. Larry Shattuck, 831-656-2473, lgshattu@nps.edu.

Statement of Consent. I have read the information provided above. I have been given the opportunity to ask questions and all the questions have been answered to my satisfaction. I have been provided a copy of this form for my records and I agree to participate in this study. I understand that by agreeing to participate in this research and signing this form, I do not waive any of my legal rights.

Signature _____ Date _____

C. **PROTOCOL APPROVAL**



Naval Postgraduate School **Human Research Protection Program**

From: President, Naval Postgraduate School (NPS)
To: Dr. Dan Boger, Graduate School of Operation and
Information Sciences (GSOIS)
CAPT Ryan Kelly, USA
Via: Chairman, Institutional Review Board (IRB)


Subj: THE EFFECTS OF SPECIALIZATION AND REFERENCE LOAD ON
INSIDER THREAT ANALYSIS PERFORMANCE

Encl: (1) Approved IRB Initial Review Protocol

1. The NPS IRB is pleased to inform you that the NPS President has approved your initial review protocol (NPS IRB# NPS.2017.0024-IR-EP7-A). The approved IRB Protocol is found in enclosure (1). Completion of the CITI Research Ethics Training has been confirmed.
2. This approval expires on 08 March 2018. If additional time is required to complete the research, a continuing review report must be approved by the IRB and NPS President prior to the expiration of approval. At expiration all research (subject recruitment, data collection, analysis of data containing PII) must cease.
3. You are required to obtain consent according to the procedure provided in the approved protocol.
4. You are required to report to the IRB any unanticipated problems or serious adverse events to the NPS IRB within 24 hours of the occurrence.
5. Any proposed changes in IRB approved research must be reviewed and approved by the NPS IRB and NPS President prior to implementation except where necessary to eliminate apparent immediate hazards to research participants and subjects.
6. As the Principal Investigator (PI) it is your responsibility to ensure that the research and the actions of all project personnel involved in conducting this study will conform with the IRB approved protocol and IRB requirements/policies

Subj: THE EFFECTS OF SPECIALIZATION AND REFERENCE LOAD ON
INSIDER THREAT ANALYSIS PERFORMANCE

7. At completion of the research, no later than expiration of approval, the PI will close the protocol by submitting an End of Experiment Report.



Lawrence G. Shattuck, PhD
Chair
Institutional Review Board



Ronald A. Route
Vice Admiral, U.S. Navy (Ret.)
President, Naval Postgraduate School

Date: MAR 10 2017

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. ITA INFORMATION PROCESS

This research initiated with a qualitative assessment of insider threat analysis organizational design. Field research informed the ITA cell organizational assignment in Figure 11 and task flow chart in Figure 12. The data from the field research informed the ITA apparatus design.

A. ITA CELL ORGANIZATIONAL ASSESSMENT

The ITA organization relationships I derived from site visits and interviews are presented in Figure 11 and formatted as an ITA process flowchart in Figure 12.

Figure 11. Analysis and Case Management Organizational Relationships.

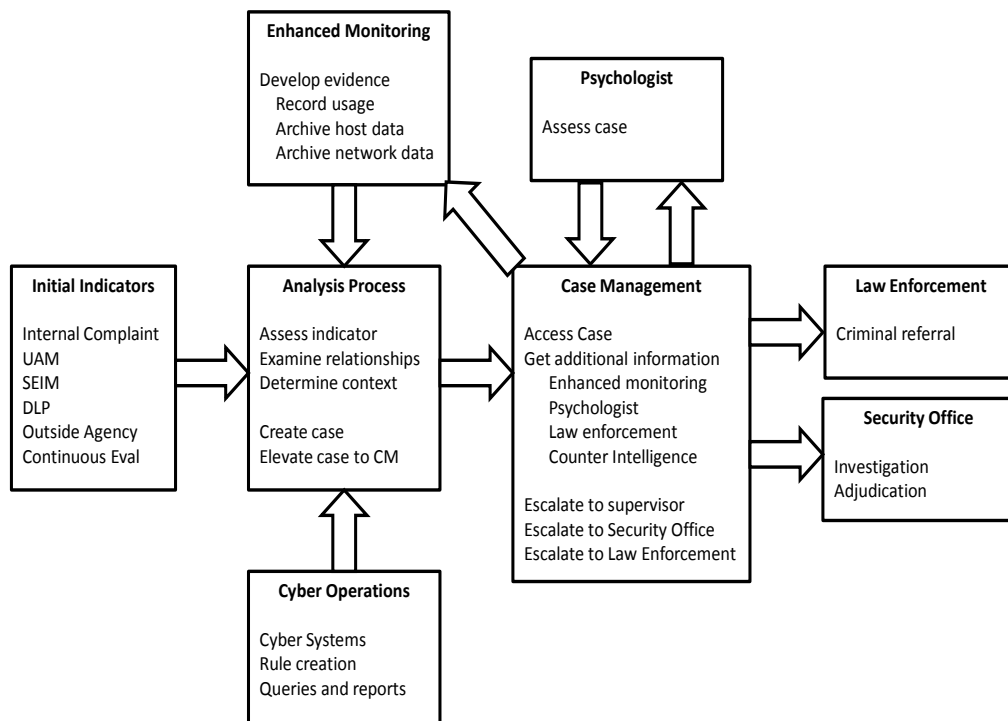
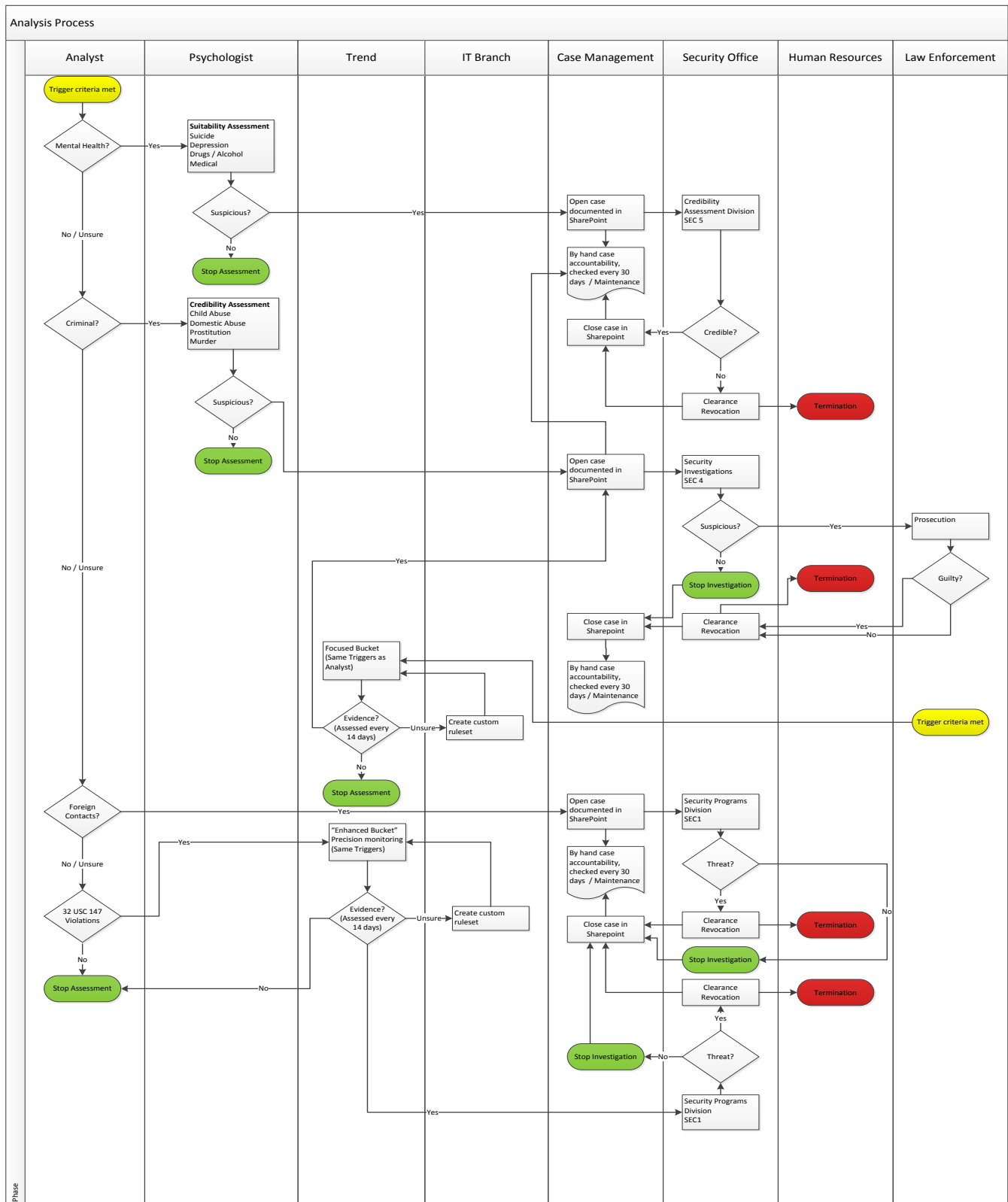


Figure 12. Insider Threat Analysis Organizational Flow Chart.



B. ITA ROLES AND RESPONSIBILITIES

ITA requires an interaction between analysts, case managers, and cyber operators. This section reports the findings from a series of qualitative interviews and observational studies.

1. Analyst

The analyst focuses on four types on insider threat activity: suitability, fraud, sabotage, and espionage.

Suitability is a function of continuous evaluation that insider threat analysts use to determine if indicators that are not work related can give the work related indicators contextual relevance. Information sources for suitability include:

- a. Mental health (depression, adultery, sexual deviancy)—Learned from email traffic, website views, medical
- b. Criminal records - Learned from federal, state, and local online reporting websites
- c. Civil court proceedings—Learned from state online reporting websites
- d. Financial / credit history—Learned from Experian, Trans-union, Equifax
- e. Drug abuse (Alcoholism, Narcotics)—Learned from self / peer reporting, drug testing
- f. Domestic violence (includes child abuse)—Learned from peer reporting, police records

When an indicator is presented in the AT—the analyst performs the following steps:

Step 1: Review related information sources to gather all indicators not explicitly defined in the AT parameters. This process is generally a quick look at each of the information sources for irregularities.

Step 2: Determine if there are things a reasonable person would assume are extra-ordinary, i.e, high credit card debt, recent divorce, large purchases, police interventions at the residence that did not result in arrest. **If none are found, stop analysis, otherwise continue to step 3.**

Step 3: Create a case: Assemble all relevant indicators into the case management software. Cases shall contain the following information:

- i. Name of subject (Last, First, M)
- ii. Status of subject (Military, Civilian, Contractor)
- iii. Demographics (pay grade, marital status, children, race, sex, claimed religion)
- iv. Date reported (DD/MM/YYYY)
- v. Date discovered (DD/MM/YYYY)
- vi. Date processed (DD/MM/YYYY) **LEAVE THIS FIELD BLANK**
- vii. Type—(Special investigation / Counter intelligence / concurrent)

- viii. Allegation—cite the contextually relevant indicator, i.e., financial problems
- ix. Predication—cite all relevant indicators (include indicator ID if in AT)
- x. Outside source—If indicators were received from an outside source, cite whom and contact information.
- xi. Classification (U, S, TS)—determined by the highest classification level of network from where indicator data was retrieved.
- xii. Name of referring analyst

Step 4: Elevate case in case management system to a case manager.

Step 5: Send a confirmation email to case manager to confirm that the case is received (if the case manager role is a different person)

- i. If case manager does not respond to the email stating that case is received within 24 hours, call the case manager and request confirmation via email.
- ii. If case manager does not answer phone, personally approach case manager and request confirmation via email.
- iii. If no case manager is available, repeat step five every 24 hours and CC the email to the hub supervisor.

Step 6: Proceed to the next complaint or indicator in the AT

Fraud is theft of resources. Fraud includes money embezzlement, clocking in when not present for hourly employees, coming in late / leaving early for salary employees, theft of property (government or personal), using government hours for personal gain (running a business from work, online gambling, excessive social media, time spent doing other things than work). Information sources for fraud include:

- a. Missing items reports
- b. Badge in / out logs (time and location)
- c. Network access logs—From security information and event management (SIEM) tool
- d. Browsing history—From user activity monitor (UAM) tool
- e. Civil court proceedings—Learned from state online reporting websites
 - i. Leans on property
 - ii. Divorce proceedings
 - iii. Foreclosure
- f. Financial / credit history—Learned from Experian, Trans-union, Equifax

When a complaint is received—the analyst performs the following steps:

Step 1: Review related information sources to gather all indicators not explicitly defined in the AT parameters. This process is generally a quick look at each of the information sources for irregularities.

Step 2: Determine if there are things a reasonable person would assume are extra-ordinary, i.e, high credit card debt, recent divorce, large purchases, police interventions at the residence that did not result in arrest. **If none are found, stop analysis, otherwise continue to step 3.**

Step 3: Create a case: Assemble all relevant indicators into the case management software. Cases shall contain the following information:

- i. Name of subject (Last, First, M)
- ii. Status of subject (Military, Civilian, Contractor)
- iii. Demographics (pay grade, marital status, children, race, sex, claimed religion)
- iv. Date reported (DD/MM/YYYY)
- v. Date discovered (DD/MM/YYYY)
- vi. Date processed (DD/MM/YYYY) **LEAVE THIS FIELD BLANK**
- vii. Type—(Special investigation / Counter intelligence / concurrent)
- viii. Allegation - cite the contextually relevant indicator, i.e., financial problems
- ix. Predication—cite all relevant indicators (include indicator ID if in AT)
- x. Outside source - If indicators were received from an outside source, cite whom and contact information.
- xi. Classification (U, S, TS)—determined by the highest classification level of network from where indicator data was retrieved.
- xii. Name of referring analyst

Step 4: Elevate case in case management system to a case manager.

Step 5: Send a confirmation email to case manager to confirm that the case is received (if the case manager role is a different person)

- i. If case manager does not respond to the email stating that case is received within 24 hours, call the case manager and request confirmation via email.
- ii. If case manager does not answer phone, personally approach case manager and request confirmation via email.
- iii. If no case manager is available, repeat step five every 24 hours and CC the email to the hub supervisor.

Step 6: Proceed to the next complaint or indicator in the AT

Sabotage is destruction of resources (includes deletion of files and rendering computer software / hardware inoperable) and “framing” other personnel. Saboteurs can be intentional or non-intentional. Information sources for sabotage include:

- a. Data / server access logs—from security information and event monitoring (SIEM) tool
- b. Review of user activity—from user activity monitor (UAM) tool
- c. Badge in / out logs (time and location)
- d. Security camera recordings
- e. Performance reviews / evaluations / missed promotions—from HR

When an indicator is presented in the AT - the analyst performs the following steps:

Step 1: Review related information sources to gather all indicators not explicitly defined in the AT parameters. This process is generally a quick look at each of the information sources for irregularities.

Step 2: Determine if there are things a reasonable person would assume are extra-ordinary, i.e, high credit card debt, recent divorce, large purchases, police interventions at the residence that did not result in arrest. **If none are found, stop analysis, otherwise continue to step 3.**

Step 3. Create a case: Assemble all relevant indicators into the case management software. Cases shall contain the following information:

- i. Name of subject (Last, First, M)
- ii. Status of subject (Military, Civilian, Contractor)
- iii. Demographics (pay grade, marital status, children, race, sex, claimed religion)
- iv. Date reported (DD/MM/YYYY)
- v. Date discovered (DD/MM/YYYY)
- vi. Date processed (DD/MM/YYYY) **LEAVE THIS FIELD BLANK**
- vii. Type—(Special investigation / Counter intelligence / concurrent)
- viii. Allegation - cite the contextually relevant indicator, i.e., financial problems
- ix. Predication—cite all relevant indicators (include indicator ID if in AT)
- x. Outside source - If indicators were received from an outside source, cite whom and contact information.
- xi. Classification (U, S, TS)—determined by the highest classification level of network from where indicator data was retrieved.
- xii. Name of referring analyst

Step 4: Elevate case in case management system to a case manager.

Step 5. Send a confirmation email to case manager to confirm that the case is received (if the case manager role is a different person)

- i. If case manager does not respond to the email stating that case is received within 24 hours, call the case manager and request confirmation via email.
- ii. If case manager does not answer phone, personally approach case manager and request confirmation via email.
- iii. If no case manager is available, repeat step five every 24 hours and CC the email to the hub supervisor.

Step 6: Proceed to the next complaint or indicator in the AT

Espionage deals with spies working for a nation state and social activists that disclose information to an unauthorized party. Espionage can be unintentional when the valid authorized access of a trusted party is compromised without knowledge. Information sources for espionage include:

- a. Data movement records—from data loss prevention (DLP) software
- b. Printing records—from print server records and user activity monitor (UAM)
- c. Data / server access logs—from security information and event monitoring (SIEM) tool
- d. Review of user activity—from user activity monitor (UAM) tool

- e. Badge in / out logs (time and location)

When an indicator is received - the analyst performs the following steps:

Step 1: Review related information sources to gather all indicators not explicitly defined in the AT parameters. This process is generally a quick look at each of the information sources for irregularities.

Step 2: Determine if there are things a reasonable person would assume are extra-ordinary, i.e, foreign travel, high credit card debt, large printing volume, high network traffic volume. **If none are found, stop analysis, otherwise continue to step 3.**

Step 3: Create a case: Assemble all relevant indicators into the case management software. Cases shall contain the following information:

- i. Name of subject (Last, First, M)
- ii. Status of subject (Military, Civilian, Contractor)
- iii. Demographics (pay grade, marital status, children, race, sex, claimed religion)
- iv. Date reported (DD/MM/YYYY)
- v. Date discovered (DD/MM/YYYY)
- vi. Date processed (DD/MM/YYYY) **LEAVE THIS FIELD BLANK**
- vii. Type—(Special investigation / Counter intelligence / concurrent)
- viii. Allegation - cite the contextually relevant indicator, i.e., financial problems
- ix. Predication—cite all relevant indicators (include indicator ID if in AT)
- x. Outside source - If indicators were received from an outside source, cite whom and contact information.
- xi. Classification (U, S, TS)—determined by the highest classification level of network from where indicator data was retrieved.
- xii. Name of referring analyst

Step 4: Elevate case in case management system to a case manager.

Step 5: Send a confirmation email to case manager asking them to confirm that the case is received (if the case manager role is a different person)

- i. If case manager does not respond to the email stating that case is received within 5 minutes, call the case manager and request confirmation via email.
- ii. If case manager does not answer phone, personally approach the case manager and request the confirmation email.
- iii. If there is no case manager available, call the security office and report what you have seen. Report that you could not get in touch with the case manager.
- iv. Send an email to the case manager and inform them that due to the severity of the incident, you have alerted security about a possible espionage case because the case manager was unavailable at the time of the incident.

Step 6: Proceed to the next complaint or indicator in the AT

2. Case Manager

The case manager evaluates cases for severity, maintains the continuity of the cases in the case management software, gathers additional information, and forwards cases to the appropriate authority.

Step 1: Open case in case management software and ensure all analyst fields were correctly populated by the referring analyst.

- a. Name of subject (Last, First, M)
- b. Status of subject (Military, Civilian, Contractor)
- c. Demographics (pay grade, marital status, children, race, sex, claimed religion)
- d. Date reported (DD/MM/YYYY)
- e. Date discovered (DD/MM/YYYY)
- f. Date processed (DD/MM/YYYY)
- g. Type—(Special investigation / Counter intelligence / concurrent)
- h. Allegation - cite the contextually relevant indicator, i.e., financial problems
- i. Predication—cite all relevant indicators (include indicator ID if in AT)
- j. Outside source - If indicators were received from an outside source, cite whom and contact information.
- k. Classification (U, S, TS)—determined by the highest classification level of network from where indicator data was retrieved.
- l. Name of referring analyst

Step 2: Complete case information in case management software

- a. HR data: Include job description, attach performance reviews
- b. Focus depth: (Enhanced monitoring / routine)
- c. Access level per network classification access: (Privileged / Elevated / Standard)
- d. Administrative remarks: A narrative record of what has been done and when.

Step 3: Determine if case is warranted for escalation or if additional information is required

- a. Does the behavior indicate a psychological problem? **Jump to step 4**
- b. Is there a minor violation of policy or minor behavior concern? **Jump to step 5**
- c. Is there a clear major violation of policy? **Jump to step 6**
- d. Is there a clear violation of criminal law? **Jump to step 7**
- e. Is the behavior questionable, but insufficient to access? **Send to enhanced monitoring with email confirmation**
 - i. If enhanced monitoring does not respond to the email stating that the case is received within 24 hours, call the enhanced monitor and request confirmation via email.
 - ii. If the enhanced monitor does not answer the phone, personally approach the enhanced monitor and request confirmation via email.

- iii. If no enhanced monitor is available, repeat **Step 3 part d** every 24 hours and CC the email to the hub supervisor.
- iv. Update “case current owner” as “enhanced monitoring” in case management.

f. **Jump to step 1.**

Step 4: Psychological problems

- a. Refer case to staff psychologist
- b. Request email receipt of referral, CC the insider threat analysis cell supervisor
- c. Request an update every 14 days, enter the information in the “administrative remarks” section of the case management software.
- d. Update “case current owner” as “psychologist” in case management.
- e. When psychologist clears the insider threat, close the case, **Jump to step 1**

Step 5: Minor threat remediation

- a. Inform supervisor and request remedial training
- b. Document the supervisor’s name, time/date, and course of action in case management “administrative remarks” record.
- c. Close case, **Jump to step 1**

Step 6: Security office referral

- a. Inform security office of the insider threat immediately by telephone
- b. Send an email with the case ID to the security office and request an email confirmation
 - i. If the security office does not respond to the email stating that the case is received within one hour, call the security office and request confirmation via email.
 - ii. If the enhanced monitor does not answer the phone, personally approach the enhanced monitor and request confirmation via email.
 - iii. If no security officer is available, repeat **Step 6 part b** every 24 hours and CC the email to the cell supervisor.
- c. Update case status every 14 days in the case management “administrative remarks.”
- d. Update “case current owner” as “security manager” in case management.
- e. After the security office clears or terminates the insider threat, close the case, **Jump to step 1.**

Step 7: Law enforcement referral

- a. Call 911 on your telephone and notify law enforcement of the crime.
- b. Record this action in the case management “administrative remarks.”
- c. Inform security office of the insider threat immediately by telephone
- d. Send an email with the case ID to the security office and request an email confirmation
 - iv. If the security office does not respond to the email stating that the case is received within one hour, call the security office and request confirmation via email.

- v. If the enhanced monitor does not answer the phone, personally approach the enhanced monitor and request confirmation via email.
- vi. If no security officer is available, repeat **Step 7 part d** every 24 hours and CC the email to the cell supervisor.
- e. Update case status every 14 days in the case management “administrative remarks.”
- f. Update “case current owner” as “security manager” in case management.
- g. After the security office clears or terminates the insider threat, close the case, **Jump to step 1.**

3. Enhanced Monitor

Enhanced monitoring is the same as analysis, but with greater focus on creating a chain of evidence for a case manager to determine appropriate courses of action. The enhanced monitoring process starts with a request for enhanced monitoring from a case manager.

Step 1: Archive all user activity in the user activity monitoring software.

Step 2: Archive all network activity in the SIEM software

Step 3: Archive all physical access (times in / out) by visual inspection if necessary

Step 4: Review emails, browsing history, keystrokes—From user activity monitor (UAM)

Step 5: Conduct full background investigation

Step 6: Annotate foreign travel (contact TSA)

Step 7: Determine if there has been any police activity (call local police)

Step 8: Civil court proceedings - Learned from state online reporting websites

a. Leans on property

b. Divorce proceedings—Read the details of the case / allegations

c. Foreclosures

Step 9: Review financial / credit history - Learned from Experian, Trans-union, Equifax

Step 10: Peer appraisals—Learned from 360 evaluation

Step 11: Maintain interactive case management

a. Report all major policy violations, criminal activity, and espionage indicators to Case Management immediately

i. If the case manager does not respond to the email stating that case is received, call the case manager and request confirmation via email.

ii. If the case manager does not answer phone, personally approach case manager and request confirmation via email.

iii. If no case manager is available, repeat **Step 11 part a** every 24 hours and CC the email to the cell supervisor.

b. Continuously update case “predication” in case management for 14 days

c. After 14 transfer case back to case management and update “case current owner” as “case management” in case management software.

4. Cyber Operator

Cyber operators maintain the security information and event management (SIEM) software, user activity monitoring (UAM) software, and data loss prevention software.

Task 1: Build rule sets by interpreting requests from Analysts and Case Managers

Task 2: Test requested rule sets for impact.

- a. New rules should not profoundly impact the number of alerts that are presented to analysts.
- b. Alerts should have a reasonable sensitivity and designed to detect a very specific behavior.
- c. Test results shall be submitted to a change control review board prior to production implementation. The change control review board should include at least one case manager role and one analyst role.
- d. Implement new rules upon approval from the change control review board.

Task 3: Review standard rule set updates to SIEM and UAM software

- a. New rules should not profoundly impact the number of alerts that are presented to analysts.
- b. Alerts should have a reasonable sensitivity and designed to detect a very specific behavior.
- c. Test results shall be submitted to a change control review board prior to production implementation. The change control review board should include at least one case manager role and one analyst role.
- d. Implement new rules upon approval from the change control review board.

Task 4: Maintain software patches for information assurance vulnerability alert (IAVA) compliance.

Task 5: Maintain access control for all insider threat mitigation cell members on information systems.

Task 6: Audit analyst and case manager access logs and report suspicious activity from analysts and case managers to the cell supervisor.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. RESEARCH QUESTION STATISTICAL ANALYSIS

This section provides the experimental data set and supporting statistical analysis outputs taken verbatim from Risk Simulator and SPSS.

A. EXPERIMENTAL DATASET

Table 46. Experiment Dataset.

Participant	Time	Accy	Perform	Conf	Info Ovld	Social Impact	Team Work	Ignor	Dispos	Scenario	Age	Gender	Edu	Exp
G1SHRLP1	753	1	1.6276	6	2	1	1	1	0	1	46	1	2	2
G1SHRLP2	873	1	1.5682	7	2	2	1	1	0	2	31	1	2	0
G1SHRLP3	666	1	1.6706	7	2	2	1	1	1	3	34	1	2	0
G1SHRLP4	853	1	1.5781	8	1	1	1	1	1	4	40	1	2	16
G1SHRHP1	1255	0	0.3793	6	2	1	1	0	0	1	79	1	2	0
G1SHRHP2	1110	1	1.4510	8	3	4	1	0	0	2	34	1	2	0
G1SHRHP3	1130	1	1.4411	6	1	4	1	0	0	3	34	1	1	0
G1SHRHP4	1209	1	1.4021	9	1	1	1	0	0	4	32	1	2	6
G1SLRLP1	635	0	0.6860	7	1		0	1	0	1	60	1	2	0
G1SLRLP2	588	1	1.7092	9	1		0	1	0	2	58	0	4	0
G1SLRLP3	578	0	0.7141	6	2		0	1	1	3	38	0	2	1
G1SLRLP4	390	1	1.8071	7	1		0	1	0	4	47	0	2	0
G1SLRHP1	846	1	1.5816	7	5		0	0	0	1	36	1	2	0
G1SLRHP2	838	1	1.5856	9	1		0	0	0	2	63	0	3	0
G1SLRHP3	894	0	0.5579	7	4		0	0	0	3	65	1	1	36
G1SLRHP4	795	1	1.6068	8	1		0	0	0	4	34	1	2	0
G2SHRLP1	628	0	0.6894	7	1	1	1	1	1	1	26	0	1	0
G2SHRLP2	758	1	1.6251	6	2	1	1	1	0	2	22	1	1	0
G2SHRLP3	1126	1	1.4431	7	2	2	1	1	0	3	34	1	1	1
G2SHRLP4	1235	0	0.3892	6	2	2	1	1	0	4	31	1	1	0
G2SHRHP1	1053	1	1.4792	8	2	2	1	0	1	1	33	1	2	7
G2SHRHP2	1626	1	1.1958	6	1	1	1	0	1	2	35	1	1	0

G2SHRHP3	1368	1	1.3234	7	2	2	1	0	0	3	27	1	1	0
G2SHRHP4	2022	1	1.0000	9	1	3	1	0	0	4	32	0	1	0
G2SLRLP1	600	0	0.7033	5	1		0	1	1	1	28	1	1	0
G2SLRLP2	480	1	1.7626	7	2		0	1	0	2	60	1	2	0
G2SLRLP3	564	1	1.7211	7	1		0	1	0	3	45	0	1	0
G2SLRLP4	468	0	0.7685	9	1		0	1	1	4	36	1	2	0
G2SLRHP1	730	1	1.6390	7	2		0	0	0	1	33	1	1	2
G2SLRHP2	810	1	1.5994	9	1		0	0	0	2	34	1	1	0
G2SLRHP3	931	0	0.5396	7	3		0	0	0	3	29	0	1	0
G2SLRHP4	1420	0	0.2977	6	1		0	0	0	4	52	1	2	2
G3SHRLP1	518	1	1.7438	5	3	3	1	1	0	1	29	1	1	0
G3SHRLP2	1004	1	1.5035	9	1	1	1	1	0	2	34	1	2	12
G3SHRLP3	757	0	0.6256	5	1	1	1	1	0	3	27	0	1	0
G3SHRLP4	943	1	1.5336	7	5	1	1	1	0	4	25	1	1	0
G3SHRHP1	1299	1	1.3576	6	1	1	1	0	0	1	37	1	2	0
G3SHRHP2	1312	1	1.3511	9	4	4	1	0	0	2	35	1	1	0
G3SHRHP3	1228	1	1.3927	7	1	2	1	0	1	3	27	1	1	0
G3SHRHP4	1989	1	1.0163	8	2	1	1	0	0	4	39	1	1	0
G3SLRLP1	434	1	1.7854	8	1		0	1	0	1	34	1	1	0
G3SLRLP2	470	1	1.7676	8	1		0	1	0	2	37	1	1	0
G3SLRLP3	513	0	0.7463	6	3		0	1	0	3	35	0	1	0
G3SLRLP4	490	0	0.7577	9	3		0	1	0	4	35	1	1	0
G3SLRHP1	767	0	0.6207	7	1		0	0	0	1	35	1	2	0
G3SLRHP2	802	1	1.6034	6	3		0	0	0	2	29	1	1	0
G3SLRHP3	1320	1	1.3472	6	5		0	0	0	3	36	1	1	1
G3SLRHP4	1260	1	1.3769	8	3		0	0	0	4	39	1	2	0

Table 47. Insider Threat Analysis Case Summaries.

Participant	Case Comments
G1SHRLP1	<p>Tom Witherspoon was spotted in Building B on Saturday afternoon for the period of 1 hour. Logged in to a TS/SCI system and printed off a document from personal drive space. Individual was carrying backpack and was seen near the shredders during before exiting the building. Individual is assigned to building A. CCTV confirmed individual matched the description of Tom Witherspoon.</p> <p>Member does not get along with supervisor and feels supervisor is incompetent.</p> <p>Would not escalate at this time without further evidence. Individual has in the past proven an excellent employee, but does not get along well with current supervisor. This may have attributed to the member coming in on weekend to complete some office tasks. If members are not supposed to be in specific buildings after hours, request review of access security policy.</p>
G1SHRLP2	<p>Curtis Quinn while on a trip to South Korea from 8–13 September 2016. Failed to report contact with local during trip debrief. Claimed he was ill one evening and was seen later that evening by coworkers. Initiated a potential insider threat. At this time I feel that this case should be elevated. This is due to several issues. First financial (failure to make loan payments, loss of spouse income). Second extended/abnormal computer usage outside of normal work hours in addition to unauthorized use of private email on government computer with suspicious individual (Angelina Em). Third The meeting with the local included paperwork and Quinn asked coworker (Leo Bryant) to keep it quiet. Fourth change in behavior becoming introvert and quiet.</p>
G1SHRLP3	<p>Payne is suspected of violating adjudicative guidelines of foreign influence and personal conduct. What Chapman reported was Payne was seen with a foreign woman out at a restaurant after calling in sick. When questioned, Payne responded “who, Tiffany?.” Tiffany is the name of Payne’s daughter...Payne is married to an oriental woman, so it is fair to say his daughter would have an exotic/foreign look to her. Payne has requested access to three different SCI programs in the last 7 weeks, however, a background investigation of him revealed nothing out of sorts. He has filed two IG complaints that haven’t been resolved. I don’t believe an investigation should be escalated on Payne at this time, however, continued monitoring should persist.</p>
G1SHRLP4	<p>Herbert Reeves was reported for suspicious activity. the suspicious activity reported is common security practices to ensure janitors do not view classified material. Herbert appears to be a below average performer according to his performance reports and peer interview. he is single and apparently looking for a female companion. he frequents dating sites and his online activity appears to coincide with the janitors visit. Additionally, the reports of him smelling of alcohol</p>

	appear that he had too good of a time over the holiday weekend and ended up having to work extra hours resulting in his lack of personal hygiene. Finally, the email address to the domain in China is likely a result of his attempts at online dating. Herbert appears to be gullible as his peer stated and probably needs to be counseled.
G1SHRHP1	I believe Witherspoon's activity on the Saturday afternoon, outside working hours, making copies, putting them in his backpack and not entering the adjacent building constitute suspicious behavior. Also, his rapid downward trend in evaluations by his supervisor cast doubt on his suitability for a TS clearance
G1SHRHP2	Curtis Q Quinn (R&D) went with a group of 6 employees on an official trip to South Korea from 8–13 September. While on the trip, Curtis had an undisclosed meeting alone with a suspected foreign national while on the trip. Previously, Curtis told his companions he was sick and unable to go to dinner with the group. 2 hours later, he was spotted by his companions in a restaurant with a female suspected foreign national with paperwork spread all over the table. Additionally, Curtis has been requesting access to classified projects of which he has no need to know. Specifically, he was given access to a COI sharepoint on missile technology. He downloaded missile technology and related information. He also had at least 3 emails from a South Korean contact, and he reportedly asked a friend to keep quiet about his South Korean contact. Curtis has also been accessing classified material well outside of normal duty hours.
G1SHRHP3	Activity and logs were consistent over long time period. Data downloaded was consistent with his data analytics job. People don't know what his wife looks like and could be the woman he had lunch with. No flags for dishonesty. Don Chapman, who reported, thought it was not really of immediate concern. Always polite and courteous with high evaluations. While I am worried about the search for "other" read-ins, I don't know if that is beyond the normal.
G1SHRHP4	Herbert Reeves has been reported for activities which may indicate he is an insider threat. Although member has not reported any foreign travel, it appears the member has frequent correspondence with a contact that may be located in China.
G1SLRLP1	Worker observed in TS/SCI workspace during period not normally authorized. No adverse indicators except recent work performance issues with supervisor. No clear evidence of wrongdoing, but anecdotal evidence warrants questioning of worker at a minimum about what he was doing on the off-work day.
G1SLRLP2	Individual was not sufficiently forthcoming about what he was doing with the woman he was seen with; the fact there was paperwork on the table remains unexplained; money is clearly a matter of concern for him; there appears to have been follow-up, cryptic email contact between an Asian woman and Quinn.
G1SLRLP3	Hector Payne

	<ul style="list-style-type: none"> -has 7 reports on dishonest and inappropriate conduct toward women -tried to access 3 different spaces requiring a clearance, need to know -has been delinquent with his credit card 2 times in the past 5 months -called in sick but was out with a female, not his wife
G1SLRHP4	Reeves was reported as acting suspiciously by janitorial staff. It is reported that this is a change in behavior. The data and reviews reveal that he has corresponded to a foreign national with an IP address associated with China. He is delinquent on a student loan for the past few month and has been accessing dating sites from work however on his lunch break. These reports raise flags of financial problems, he has reported to co-workers that he is working weekends, but does not want credit and has connection with a foreign entity. He has access to several SCI programs and may be vulnerable to share information for money.
G1SLRHP1	The main flag is that he printed 276 pages of something from a classified terminal in a building that was not his on a weekend. It is very possible that he took some of the papers in his backpack. There are not really other indicators in his personal files that would flag him as insider threat. Not liking his boss is not unusual. Probably worth looking into to find out what the document was and where he took it. May want to wait to see if it happens again.
G1SLRHP2	<p>A little torn on whether to refer but decided in favor of referring for following reasons:</p> <ol style="list-style-type: none"> 1. Actions on trip where he ended up at dinner with unknown Korean female and papers on table. Note that he did not admit to this until confronted about it. Initially denied saying he was sick. 2. Only member of group with e mail contacts in South Korea. 3. Financial issues (late mortgage payments) possibly due to wife having lost her job. 4. Several attempts to gain access to programs for which he had no need to know, among them Fireball. 5. Attempt to access info on Fireball sideways through speaking with coworker.
G1SLRHP3	Reports of Payne associating with possible foreign nationals at Bellismio restaurant. Times unaccounted for on numerous occasions - Long times badging between office and outer door. Dissatisfaction with agency and policies
G1SLRHP4	Mr. Reeve's initiated an online relationship via a dating website with a foreign citizen and maintained regular communication. Digital records of this communication indicate that he regularly discussed sensitive (possible classified) portions of his job with this person. Passport records and digital communication indicate that Mr. Reeves made an undisclosed trip to Malaysia to visit the foreign citizen. Mr.s Reeve's low performance, financial issues, general naivety, and disclosure that he was breaking company policy to make the trip make him a great target for blackmail.
G2SHRHP1	Tom Witherspoon reportedly seen by CCTV cameras as well as eye witness Sam Clemens (worked in building B for more than 4 years) entering building B (when he works in building A) with a black backpack. Sam Clemens reportedly witness Tom Witherspoon, acting nervous at a TS/SCI computer printing a document. The document was found out to be

	<p>a 276 document labeled S//NF.tomswork located in the S drive in tom's stuff folder and it is password protected. Sam Clemens witnessed Tom putting documents in his backpack and shredding documents with the classified shredder. Sam Clemens did not see Tom Witherspoon leave. In the HR personnel data review his recent review went from a 4.5 last year to a 2.5 due to insubordination and untruthfulness protocol. In the continuous evaluation, no suspicious behavior was found. A peer interview stated that his friend was not aware of any new projects or weekend work hours. He did state that Tom liked printing documents, rather than looking at it on a computer for review in policy and guidelines. He said he has never seen Tom carry a backpack. Recently he has stated that Tom has had issues with the supervisor, feeling that the supervisor is incompetent and felt he was being singled out all the time. His behavior on the weekend is very suspicious.</p>
G2SHRLP2	<p>I suspect that Curtis Quinn is involved in selling information or technologies from his workplace to an outside entity without permission for financial gain to help support his family after his wife lost her job last summer. He is badging in at odd hours and requesting access to new programs to find something of interest to the talent agency he is trying to sell to. He has communicated with them over email and now with an in person meeting during the South Korea trip.</p>
G2SHRLP3	<p>Coworker who does not like Hector Payne has submitted reports of Hector meeting with a foreign contact who as it turns out is most likely his wife. The only areas that appear questionable would be his two financial late payments on his credit card accounts. This easily can be explained by his wife needing a lot of medical assistance.</p>
G2SHRLP4	<p>According to co-workers, Herbert Reeves has been acting differently for the last two weeks. A co-worker, C. McCarthy, Reeves has developed an attitude and has smelled of alcohol. Additionally, the custodian has reported strange behavior regarding computer usage, all incidents occurring at work. Based on reported activity, it is likely the custodian walked in on Mr. Reeves while he was on an adult dating website. He has contact with a foreign national through online dating sites; however, it is likely unknowingly as he has been reported as a smart but gullible guy. Based on his profile and the information, it appears as though he likes to drink and have a good time and may be subject to additional investigation in relation to Guideline G and E, but he is unlikely to be willfully engaged in illicit or damaging activities. I recommend counseling; training; and further monitoring, but not further escalation at this time.</p>
G2SHRHP1	<p>Tom Witherspoon was seen printing 278 pages of documents in a BLDG (BLDG A) that he did not work in on September 18, 2016 @ approximately 1330. Building access reports indicate that he entered the BLDG from 1300 - 1400. The documents were determined to have originated from a secret server and the document was named, "Secret//NOFORN_Tom's Work doc." This file was in subfolder "Policy, Oversight, and Management." Witherspoon has an ambivalent relationship with his supervisor and is currently in the process of appealing a bad review. Witherspoon has previously had a excellent reports and his co-workers do not report behavior that is consistent with someone attempting to deceive the U.S. Government or commit espionage.</p>

G2SHRHP2	<p>Who, Quinn</p> <p>What, possible foreign contacts, disclosing files and papers to foreign national, financial troubles, requesting access to governments</p> <p>Where, at work and during an official trip to S. Korea</p> <p>Why, he is asking for areas outside of his specialty, he met with a female foreign national, suspicious behavior and introverted.</p> <p>How: Foreign influence, Financial considerations, and emotional/mental/personality disorders.</p>
G2SHRHP3	<p>Hector Payne is a high performer that is consistently late and has created some inter-personal issues within the office. His wife has been ill for a prolonged period of time, which may be a factor in his consistent tardiness to work. Recently, a suspicious incident occurred and was reported by his co-workers. It appears he called in sick to work, but was observed outside of work with a foreign-looking female. When questioned about this female, he responded, “Who Tiffany?” and laughed. He has a daughter named Tiffany, and a wife with a name that stands out as distinctly Asian. This could be a simple father-daughter date.</p> <p>He has had two delinquencies on credit card bills, but does not seem to be enough of a pattern to be of concern. He was denied access to three compartments, but he is a part of a high-priority project and could be seeking out ways to enhance it.</p> <p>Altogether, these factors do not seem to warrant escalation.</p>
G2SHRHP4	<p>Mr. Herbert Reeves has been reported to have changes in behavior by multiple people, all of which have been substantiated by unreported travel to Malaysia, failure to pay bills, unreported foreign contact, possible misuse of alcohol, and overall questionable judgement. All of this has been occurring over the past 3 months. His intentions are unclear, but it is obvious that Mr. Reeves is demonstrating a pattern of suspicious behavior.</p>
G2SLRLP1	<p>Tom Witherspoon has been observed printing a 276 page document titled S//NF_Tom’s Work.doc in the copy room of building B at XYZ agency. This took place during a non-work day (Saturday) from roughly 13–1400.</p> <p>Factors of consideration:</p> <ul style="list-style-type: none"> -Has a copy room in his own building, though it’s not as large. -Nervous, so knowingly breaking the rules, but it could be personal use that has him nervous, i.e., missing dog flier. -Good salary, but has 4 dependents, which could create a financial burden. -Recent drop in performance compared with historical yearly reviews. Possibly connected to conflict with supervisor and

	<p>not actual performance.</p> <p>-Cited for non-compliance in the past, adds to the possible personal use of the copy facilities.</p> <p>-The document that was printed had been classified by the individual as Secret NF, indicating that he knew that his document was sensitive.</p>
G2SLRLP2	<p>Wife lost job.</p> <p>Experiencing money problems</p> <p>Late on last several months mortgage</p> <p>Lied to coworkers to avoid going out with them</p> <p>met an unknown female at a restaurant</p> <p>Did not report the meeting of female, possibly foreign national</p> <p>asked about programs he did not have clearance for and had been denied access to</p> <p>demeanor at work has changed recently</p>
G2SLRLP3	<p>I do not believe this should be elevated for the following reasons:</p> <p>-Employee performance has been steadily increasing (3.5, 4, 4.5)</p> <p>-No CI flags</p> <p>-No Passport Flags</p> <p>-2 late credit card payments not highly unusual</p> <p>-The Badging in/out outside normal office hours could be explained (Payne assigned or taking on additional work for colleagues, or escape mechanism to deal with his wife's illness)</p> <p>-No unusual system activity</p> <p>-2 IG complaints not overly suspicious</p> <p>-Multiple requests for access to compartmented programs (SKYEYE, OBSERVER & ROSETTA) is mildly concerning because he clearly doesn't have a demonstrable "need to know" - if he had a legitimate need to know to perform additional tasks, Mr. Payne's supervisor should have initiated the request for access.</p> <p>-Banking records do not show any recent/unexplained affluence (he's late on his credit cards payments as recent as three months ago) -but could also be an indication of increasing financial problems. Wife is ill, so medical bills could be mounting. Keep an eye on this.</p>
G2SLRLP4	<p>I do not believe that Mr Reeves requires further investigation due to the fact that his behavior and further information from the XYZ agency revealed that he is most likely involved in some Internet dating. While his most recent communication seems to with a Chinese national, I do not believe that he should be considered an insider threat. Mr Reeves also has had some previous incidents with tardiness and accusations of alcohol use however, these incidents do</p>

	not point toward an insider threat. Furthermore, his work relationship with the janitor seems to be rocky due to previous conflicts and I believe his report might be somewhat biased because of this.
G2SLRHP1	The suspect had lawful access to the facility and worked regularly with TS SCI material.
G2SLRHP2	Quinn was on a business trip to South Korea recently for a period of about five days. One night during the trip, Quinn claimed to be sick and declined going to dinner with his colleagues. Later that night, his colleagues saw him at a nearby restaurant eating dinner with a Korean woman with papers in between them on the table. Quinn did not mention this interaction on his travel debrief and told his colleagues the meeting was nothing. However, Quinn has been acting strange recently. At various times over the past three months he has been accessing the SCIF at odd hours, requesting to access compartmented programs for which he does not have a “need to know” and has been in intermittent contact with someone from South Korea via email. Additionally, he received an email from a contact that asked for an item of “mutual interest.” Of note, Quinn has also been behind on his mortgage for the past three months. While Quinn is an exceptional performer for agency XYZ, there appears to be too many indicators of suspicious behavior not to look into this further.
G2SLRHP3	I feel that there is an issue to be investigated further due to the recent financial issues Payne has had which coincide with recent denied requests for read in on TS/SCI information and observed behavior not consistent with known personality. His appearance at a party with an unknown female who brushed off association with when asked, should be considered a behavioral flag.
G2SLRHP4	Below average, new, low level Network Systems Administrator, with new TS/SCI clearance has made undisclosed foreign travel to Malaysia. Subject is single and actively dating. Foreign travel appears to be benign... a trip to visit a woman. Employee is habitually late: Recommend further counseling from HR and Supervisor. Employee has apparent personality conflicts with coworkers: Recommend team building exercises. Employee executed foreign travel without disclosure: Recommend Counseling from Security Manager. Employee has access to numerous security compartments: Recommend limiting access to just a few projects.
G3SHRLP1	Who: Thomas Witherspoon What: Seen by fellow employee printing off TS-SCI documents and placing them in a backpack. Where: Building B (Witherspoon only works in Building A) Why: CCTV showed entering and leaving building B with a black backpack; he did not enter building A. The parking lot is not monitored. How: No other indicators outside this one incident. Appears to be due to improper training or inadequate training and was isolated/infrequent in nature

G3SHRLP2	<p>Who: Quinn What: Undisclosed meeting with foreign personnel Where: S. Korea Why: Quinn did not attend a team dinner but instead stated he was sick and returned to his hotel room. He was later located at a restaurant with an unnamed Asian Female with unknown papers on the table. He stated that he took medicine, felt better, went to dinner and was paired with the Asian Female at the same table. He further stated that he did not mention this during the debrief because he did not want to upset his wife. Prior to the trip he received an email from Talent Agency International Models, Inc, on Aug 19, 2016, stating “I trust that your search for our item of mutual interest is going well. Very much look forward to connecting soon.” It was signed “Angie.” The country code in the phone number was from Singapore. This contact was also not disclosed to the SSO.</p> <p>When combining Quinn’s 4x missed mortgage payments, foreign email contact, undisclosed foreign meeting in Korea, his attempting to access 2x programs for which he didn’t have a need to know, and his preference to lie to family rather than explain why he had dinner with a female, he meets the requirements for further investigation.</p>
G3SHRLP3	<p>Hector Payne is a good worker but is very outspoken about his disagreement with his organization’s mission. His filing two IG complaints and requesting access to special programs are red flags in terms of insider threat. Additionally, his request for access to additional programs came shortly following two delinquent credit card payments, which brings some questions as well. Payne is being reported for contact with a possible female foreign national, which may/may not be his wife. While there are no direct indications that he is an active insider threat, it may be necessary to conduct an investigation into Mr. Payne.</p>
G3SHRLP4	<p>Possible security risk due to personal behavior changes, financial difficulty, poor performance scores, and unreported foreign contact.</p> <p>Low performance and personality changes do not, by themselves, constitute a security risk, but changes in personal conduct, recent student loan payments, potential alcohol abuse, and foreign contact that was unreported leave subject open to blackmail.</p>
G3SHRHP1	<p>Tom Witherspoon accessed BLDG B at 1302 on 18 SEP (weekend), logged into terminal sci00037 with own login ID at 1348, printed 276 pages. Departed at 1410 with backpack and did not go to BLDG A (his normal workspace). File printed appeared to be Tom’s, located on a share drive, and cannot be determined to actually be classified. Normally works M-F, normal hours, prefers printouts. Decline in performance evaluation and abrasive attitude towards co-workers and supervisor is cause for concern.</p>

G3SHRHP2	<p>Quinn, Curtis is suspected of questionable behavior that suggest insider threat.</p> <p>Quinn failed to report foreign contact while attending a trip to South Korea, this is of concern due to describing the encounter to his co-workers as being coincidental, however, his pre-trip work behavior show him corresponding with South Korean IP addresses. Quinn also shows a pattern of behavior to include financial irresponsibility, and consistent attempt to access classified material which is outside the purview of his need to know.</p>
G3SHRHP3	<p>Hector Payne was observed with at a restaurant with a woman (possibly foreign) who was not his wife and acting in a very familiar manner with said woman. Review of all available records regarding Payne returned the following finding: When confronted about the incident with the woman, Payne did not deny the incident and only laughed off the details of his specific relationship.</p> <p>There is no definitive information which points to the woman being a foreign national.</p> <p>His IP records do not indicate any correspondence with foreign IP addresses.</p> <p>Payne is a solid performer.</p> <p>Payne, though outspoken has demonstrated a willingness to work inside agency channels to resolve any concerns.</p> <p>Has been delinquent on two credit card payments but no egregious concerns regarding finances.</p> <p>He did request access to thee compartments and was denied access due to lack of need to know. This is of concern but not a definitive flag for insider threat behavior.</p>
G3SHRHP4	<p>Mr. Herbert Reeves was recently reported to have displayed increasingly odd behavior.</p> <p>There is evidence showing that he has been making contact with a certain leimei on a Chinese-hosted website (China UNICOM: 218.60.56.105). This contact started via online dating. There is also evidence of unreported travel to Malaysia to see this foreign agent over Labor Day weekend (1-5 SEP). Furthermore, their emails indicate they have discussed his work.</p> <p>There is also a flag on his finances that shows he is now three months delinquent on his student loan payments.</p> <p>These are significant indicators to suggest Mr. Reeves has violated guidelines for maintaining his clearance.</p>
G3SLRLP1	<p>Tom Witherspoon was suspected of improperly accessing or handling TS/SCI material on a weekend in a building in which he does not normally work. I am not escalating because, in the peer interview, his friend stated that Tom's supervisor was singling him out for additional work. This may account for the poor mark on his last performance review as well as the weekend work. Additionally, printing a large volume of paper is not unusual, especially given the comment by Tom's friend, and appearing nervous is not necessarily grounds for escalation. Working in a different building on a weekend is enough to make most people uncomfortable and may account for the change in behavioral patterns. Finally, the background review did not indicate any red flags such as financial trouble or domestic problems.</p>

G3SLRLP2	<p>Who: Curtis Quinn What: Foreign Influence Where: South Korea Why: Issues with delinquent payments How: Email from personal email on a government computer to an foreign “talent agency.” The information in the email was vague.</p> <p>Last minute change of plans due to sickness and then immediately feeling better. Did not try and meet up with own group.</p> <p>Did not disclose foreign contact to associates or to SSO. This contact was not a part of his official travel. Wanted to keep meeting secret because of his wife.</p> <p>Had requested information on several programs recently that he did not have a need to know and also was trying to get more information out of associates on programs they were read into.</p>
G3SLRLP3	<p>Based on the strange office hours as identified by badge tracking, coupled with requests for clearance/access to programs (all three of which were denied) and the dishonesty IRT skipping work all lead me to believe that an investigation should take place. The only piece of evidence that would make me believe that all events are merely circumstantial and more related to his wife’s illness is the coincidence of the conversation with his employee who referenced “Tiffany” who coincidentally is his daughter as well. Nonetheless, there are too many instances that appear suspect, which outweigh the single instance of possible coincidence.</p>
G3SLRLP4	<p>M. Reeves is suspected of activities that raised security concerns from the sanitation worker (Aubrey?)and hos co-worker (McCarthy)?</p> <p>I believe there should not be an investigation on Reeves. He is acting “squirrely” because he is going on websites that are inappropriate for the workspace (his actions are against the IA and computer user agreement form he signed to get access to network resources).</p> <p>He will be more on-guard specially since going to websites “like adult friend finders and Ashley Madison” are embarrassing . His interaction with a foreign woman “MeiLei” is not unexpected since this could be a person looking for love in another country or part of a scam.</p> <p>His suspected smell of alcohol after a holiday raises questions about alcohol dependency or abuse but this seems to be his only reported incident in two years. Also only his co-worker (who does not get along with Reese) is the only person that reported it.</p>

	<p>His delinquency on his student debt raises concerns about his financial state and should be addressed. These are fairly recent and the SSO is aware of the missed student loan payments. My recommendation is to have Reese go to the financial counselor for counseling.</p> <p>Mr. Reese is just looking for love using the wrong resources (work computer), possibly partied too much one weekend, and is delinquent on just three student loan payments. The fact that he does not have the best personality makes him unpopular in the office. He does not warrant an investigation.</p>
G3SLRHP1	<p>Who: Tom Witherspoon What: Possible Insider Threat Where: Building B How and Why: Tom Witherspoon was seen on the weekend printing large amounts of material and placing them in a black backpack. He then departed the building. He does not normally work in Building B or on the weekends. He is not known to carry a black backpack to work, although he is known to prefer printing over reading on the computer. His performance has declined and his most recent evaluation marks were at 2.5 when all others were above a 4. His behavior has changed and his supervisor has noted that he has become defiant and confrontational. He has also started coming to work late and leaving early in addition to his unexcused absences.</p>
G3SLRHP2	<p>Curtis Quinn appears to possibly be involved in stealing and sharing or selling sensitive information to a foreign national. Mr. Quinn has a recent history of requesting access to programs without a need to know, is delinquent of financial obligations, accessing work buildings outside of normal business hours, and was observed interacting with a foreign national on a business trip. Mr. Quinn lied about the contact. Mr. Quinn is a top performer at work, but is recent behavior suggests there may be a security concern.</p>
G3SLRHP3	<p>Mr. Payne has a TS/SCI clearance and has had access to CI for work. General characterization of his demeanor is reclusive and occasionally grumpy. Payne seems to take pride in his work but reluctant to socialize or involve peers with group work.</p> <p>The incident in question is the result of a colleague seen with an attractive female that appears to be foreign. Additional aggravating factors that raise concern for security is that Payne has been delinquent on two credit card payments, and recently denied CI access to three programs although dates denied to access are difficult to corroborate with other events. Additionally, Payne spent an extra hour in BLDG A, but not in room 222 which is where he normally works. Typical days have Payne entering BLDG A, then taking about 3–5 minutes transit time to reach the location in room 222. On 2</p>

	<p>Sep, Payne spent an extra hour in the building that appears to be unaccounted for. This may be explainable but warrants further explanation. The day prior to the extra hour, Payne received an email from an South Korea, and previous emails from same person exist. Again, may not be a factor, but worth looking into to determine if further investigation is required.</p> <p>Mitigating factors include that Payne and woman in question were dining at a public restaurant, in Payne's hometown. Neither party seemed to hide that they were dining together. Payne did not volunteer information about the event but this matches his general non-social behavior. Colleagues description about female in question were that she looked like a foreign national. The female may not be a foreign national, and because of Payne's wife's background, and activity occurring publicly and in his hometown, the activity does not seem suspicious.</p> <p>Considering the information available, I would like to ask a few questions to clarify information available, but do not feel further investigation is warranted.</p>
G3SLRHP4	<p>In this case Mr. Herbert Reeves was reported by a Ms. Aubrey McBride for "suspicious activity."</p> <p>After reviewing the provided information I believe a formal investigation on Mr. Reeves is warranted.</p> <p>He has been hiding a romantic relationship with a foreign national (woman) that claims that she is from Malaysia, but her IP address is registered to China Unicom Laoning. Additionally, he recently made a trip to Malaysia to meet up with this woman and did not report his travel.</p> <p>Mr. Reeves co-workers reported him to be gullible, which the foreign national woman may be using to get closer to him and eventually phish for more information regarding Mr. Reeves job. It seems like he already provide some details of what he does on the job during their recent encounter in Malaysia.</p> <p>Lastly, Mr. Reeves has been late making payments on his student loans, which could be used as leverage if his debt is large. This could establish a pattern of not meeting financial obligations</p>

B. DISTRIBUTIONAL FITTING

Table 48. Distributional Fitting.

Time			Accuracy		
Fitted Distribution			Lognormal		
Mean			944.33		
Standard Deviation			418.68		
Kolmogorov-Smirnov Statistic			0.06		
P-Value for Test Statistic			0.9965		
Actual			Theoretical		
Mean			923.71		
Standard Deviation			384.12		
Skewness			0.95		
Excess Kurtosis			0.84		
Fitted Distribution			Cosine		
Minimum			1.00		
Maximum			1.00		
Kolmogorov-Smirnov Statistic			0.29		
P-Value for Test Statistic			0.0004		
Actual			Theoretical		
Mean			0.71		
Standard Deviation			0.46		
Skewness			-0.95		
Excess Kurtosis			-1.15		
Performance			Confidence		
Fitted Distribution			Gumbel Minimum		
Alpha			1.45		
Beta			0.36		
Kolmogorov-Smirnov Statistic			0.15		
P-Value for Test Statistic			0.1910		
Actual			Theoretical		
Mean			1.25		
Standard Deviation			0.46		
Skewness			-0.68		
Excess Kurtosis			-1.01		
Fitted Distribution			Weibull 3		
Location			5.00		
Alpha			1.47		
Beta			2.68		
Kolmogorov-Smirnov Statistic			0.17		
P-Value for Test Statistic			0.1250		
Actual			Theoretical		
Mean			7.17		
Standard Deviation			1.19		
Skewness			0.14		
Excess Kurtosis			-0.87		
InfoOvid			Confidence		
Fitted Distribution			Cauchy		
Alpha			1.57		
Beta			0.53		
Kolmogorov-Smirnov Statistic			0.24		
P-Value for Test Statistic			0.0065		
Actual			Theoretical		

1. Tests of Normality

This research assessed six dependent variables for normality—performance, time, accuracy, confidence, information overload, and social impact—using Kolmogorov-Smirnov and Shapiro-Wilk tests. The data from all but one dependent variable was not

normally distributed, which indicates that non-parametric tests are required to assess differences between groups (Kerlinger & Lee, 2000). General consensus holds statistical significance when $p < .05$, but tests of normality are opposite. The null hypothesis for the Kolmogorov-Smirnov test states that the data fits a normal distribution. Thus, a high p value indicates the data follows a normal distribution. Results from the normality tests are listed in Table 49.

Table 49. Tests of Data Distribution Normality.

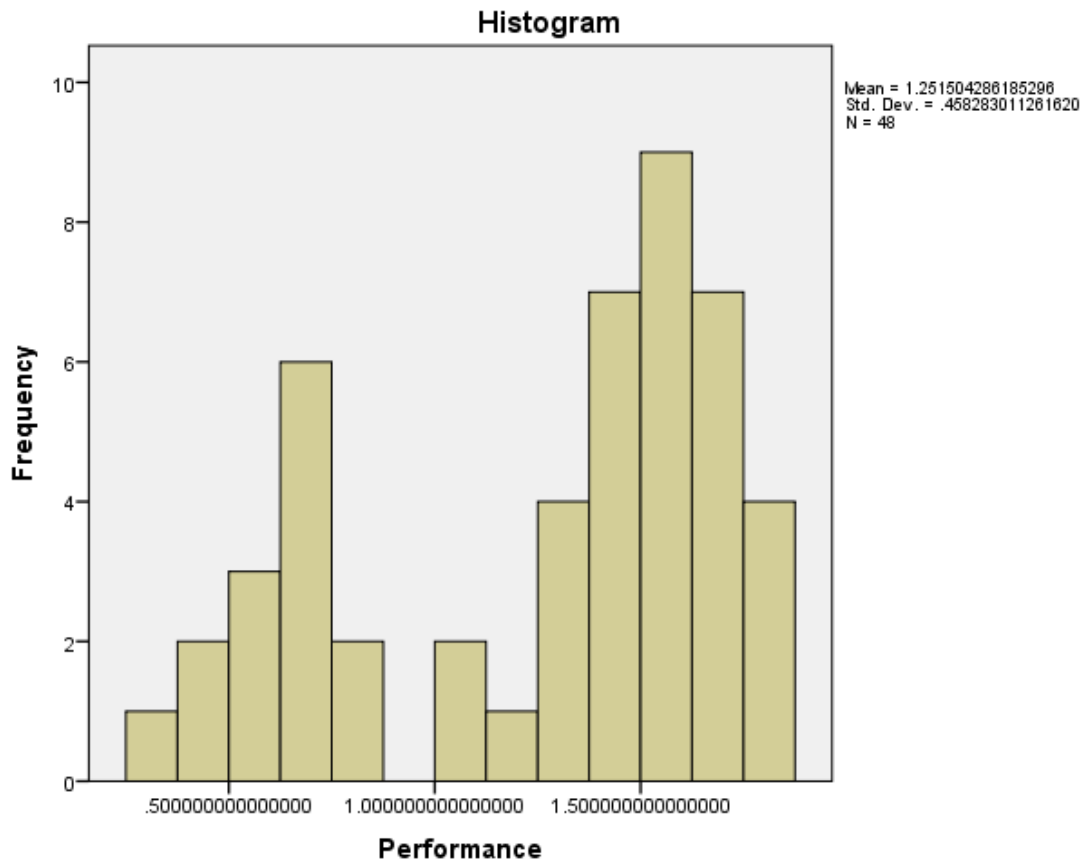
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Performance	.249	24	.000	.835	24	.001
Time	.136	24	.200*	.933	24	.111
Accuracy	.503	24	.000	.454	24	.000
Confidence	.180	24	.043	.909	24	.034
InfoOvld	.285	24	.000	.770	24	.000
SocImpact	.286	24	.000	.759	24	.000

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

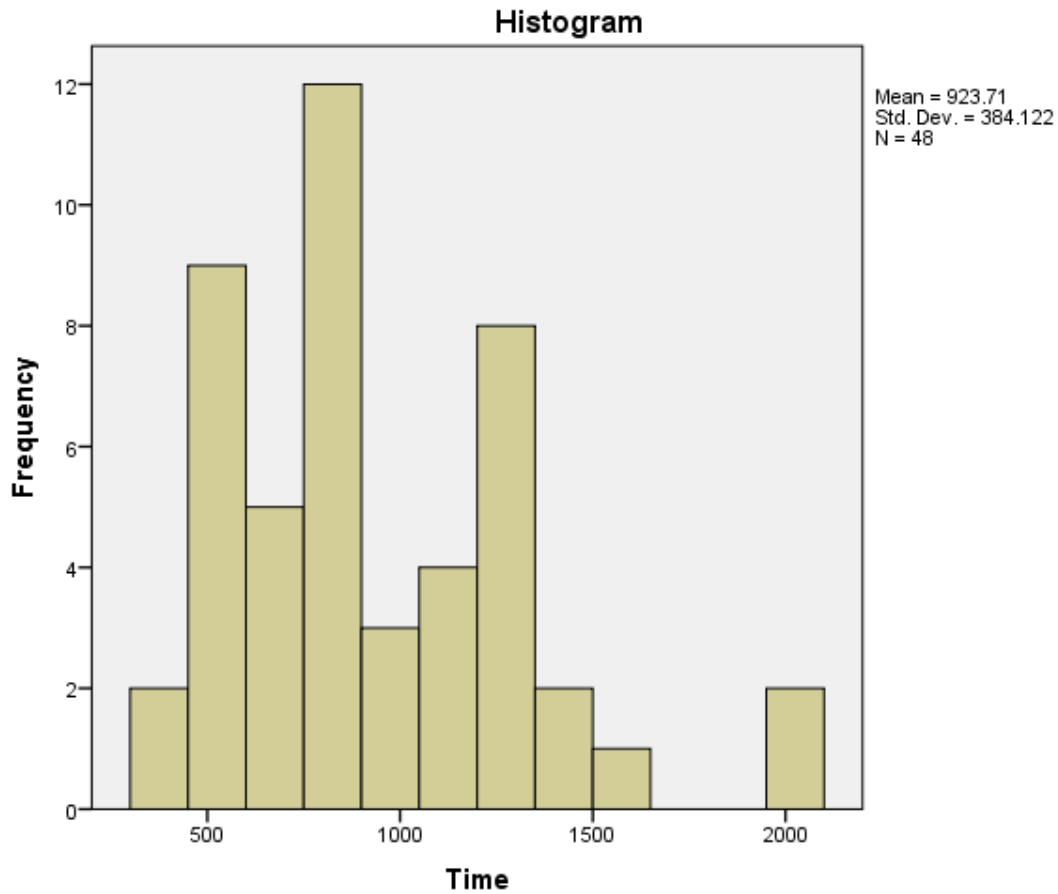
ITA performance is comprised of a rank-transformed time component and a binary accuracy component. Performance values follow a bimodal distribution when the accuracy data reflects both correct and incorrect analyses. Performance was distributed between .298 and 1.807, a range of 1.509 ($\mu = 1.25$, $\sigma = .458$). According to both the Kolmogorov-Smirnov and Shapiro-Wilk tests for normality, performance is not normally distributed ($p < .05$). Figure 13 is a visual representation of the bimodal performance data distribution.

Figure 13. Performance Data Distribution.



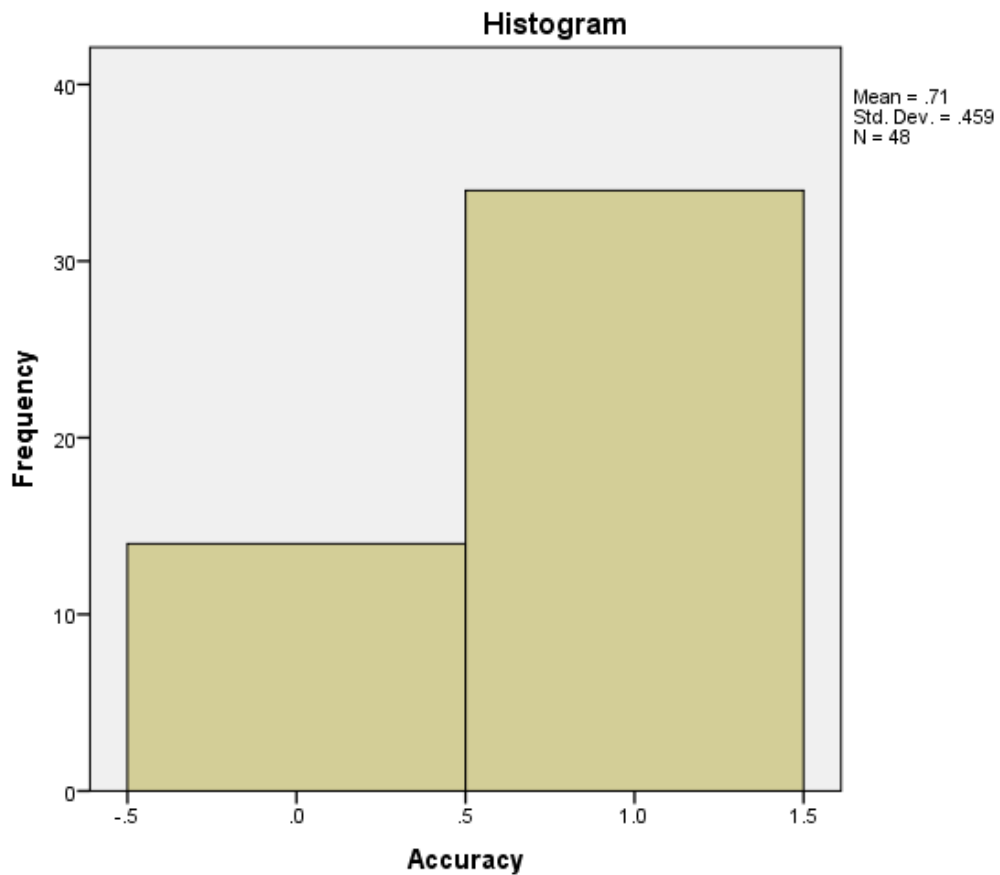
ITA time data was distributed between 390 and 2022 seconds, a range of 1632 seconds ($\mu = 923.71$, $\sigma = 384.12$). ITA time data was normally distributed according to the Kolmogorov-Smirnov and Shapiro-Wilk test for normality ($p < .05$). Figure 14 is a visual representation of the time data distribution.

Figure 14. Time Data Distribution.



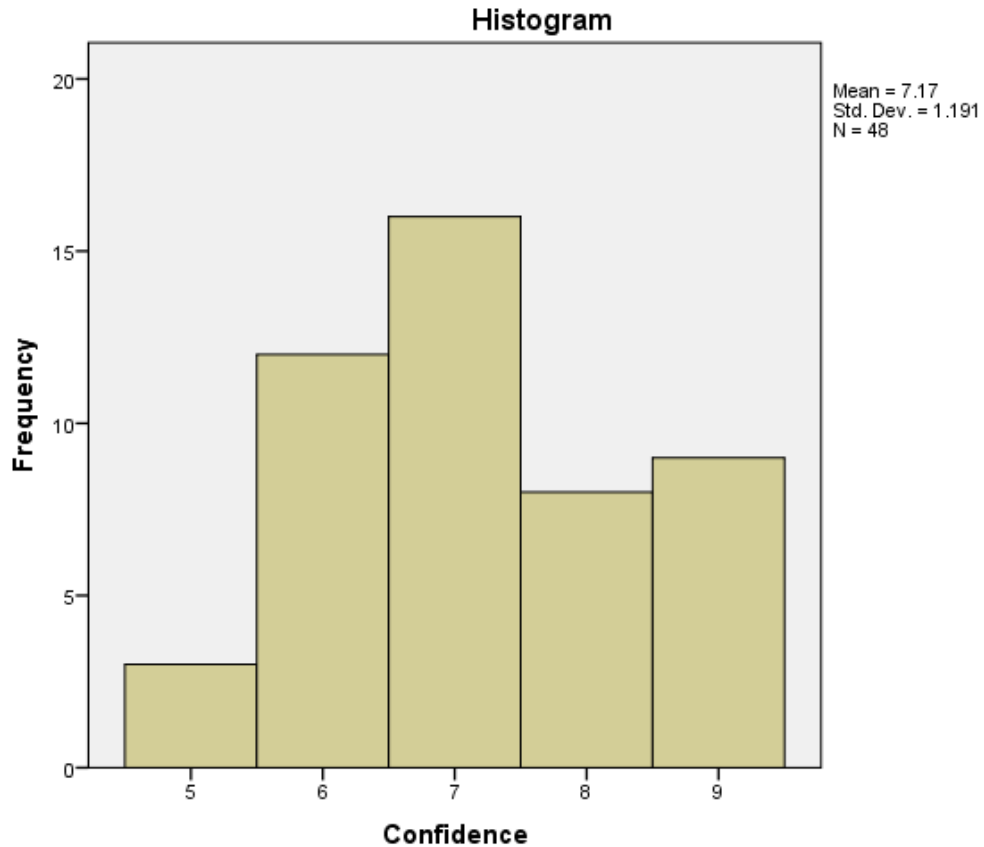
ITA accuracy was distributed between two values: 0 and 1 ($\mu = .71$, $\sigma = .459$). 34 participants performed a correct insider threat analysis and 14 performed an incorrect analysis. Figure 15 is a visual representation of the accuracy data distribution.

Figure 15. Accuracy Data Distribution.



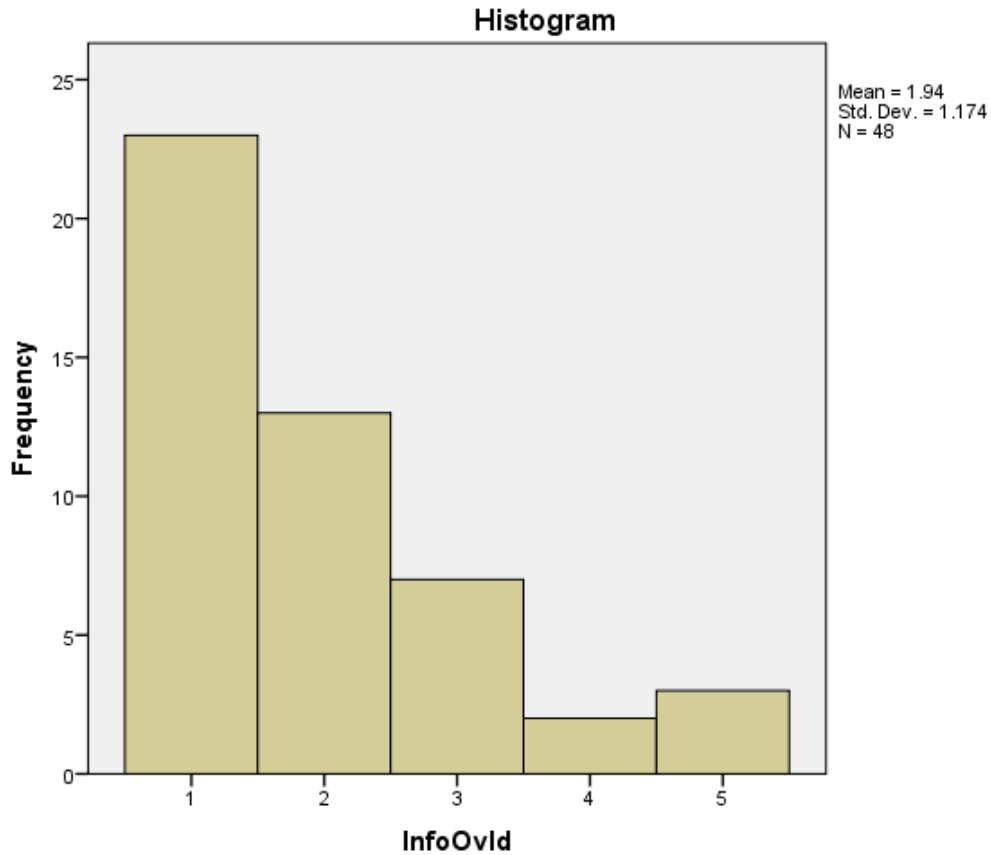
Confidence was distributed between 5 and 9 ($\mu = 7.17$, $\sigma = 1.191$). According to both the Kolmogorov-Smirnov and Shapiro-Wilk tests for normality, the confidence data does not fit a normal distribution ($p < .05$). Figure 16 is a visual representation of the confidence data distribution.

Figure 16. Confidence Data Distribution.



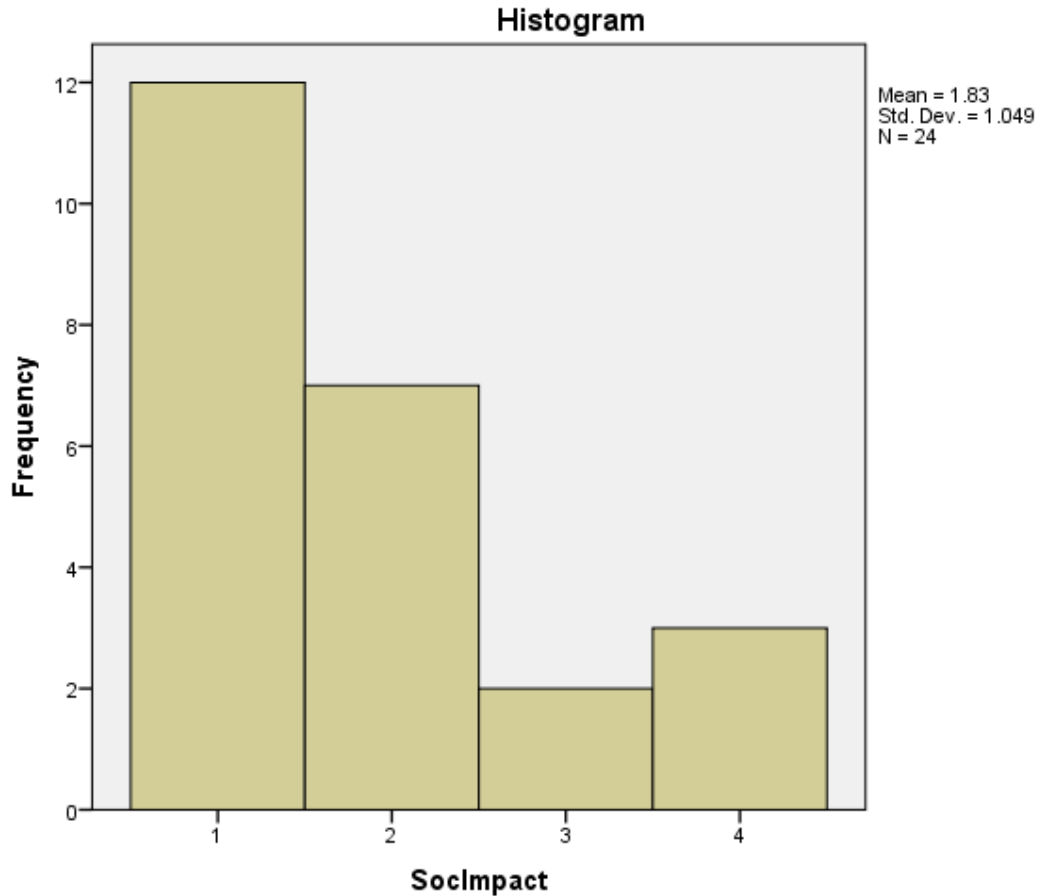
Information overload ranges from 1 to 5 ($\mu = 1.94$, $\sigma = 1.174$). According to both the Kolmogorov-Smirnov and Shapiro-Wilk tests for normality, the information overload data does not fit a normal distribution ($p < .05$). Figure 17 is a visual representation of the information overload data distribution.

Figure 17. Information Overload Data Distribution.



Social impact ranges from 1 to 4 ($\mu = 1.83$, $\sigma = 1.049$). According to both the Kolmogorov-Smirnov and Shapiro-Wilk tests for normality, the social impact data does not fit a normal distribution ($p < .05$). Figure 18 is a visual representation of the information overload data distribution.

Figure 18. Social Impact Data Distribution.



2. Tests of Homoscedasticity

Heteroscedasticity is common in cross-sectional data (Long and Ervin, 2000). This research does not evaluate time-series data; thus, homoscedasticity is not applicable for ITA performance, accuracy, confidence, and perception of information overload. This research used Levene's test for Equality of Error Variances to determine that the time data is not homoscedastic ($p < .05$). The results from Levene's test are in Table 50.

Table 50. Levene's Test for Equality of Error Variances.

Dependent Variable: Time			
F	df1	df2	Sig.
3.998	3	44	.013

Tests the null hypothesis that the error variance of the dependent variable is equal across groups.

a. Design: Intercept + Team + Ign + Team * Ign

C. DESCRIPTIVE STATISTICS

Almost all distributions can be described within 4 moments (some distributions require one moment, while others require two moments, and so forth). Descriptive statistics quantitatively capture these moments. The first moment describes the location of a distribution (i.e., mean, median, and mode) and is interpreted as the expected value, expected returns, or the average value of occurrences.

The Arithmetic Mean calculates the average of all occurrences by summing up all of the data points and dividing them by the number of points. The Geometric Mean is calculated by taking the power root of the products of all the data points and requires them to all be positive. The Geometric Mean is more accurate for percentages or rates that fluctuate significantly. For example, you can use Geometric Mean to calculate average growth rate given compound interest with variable rates. The Trimmed Mean calculates the arithmetic average of the data set after the extreme outliers have been trimmed. As averages are prone to significant bias when outliers exist, the Trimmed Mean reduces such bias in skewed distributions.

The Standard Error of the Mean calculates the error surrounding the sample mean. The larger the sample size, the smaller the error such that for an infinitely large sample size, the error approaches zero, indicating that the population parameter has been estimated. Due to sampling errors, the 95% Confidence Interval for the Mean is provided. Based on an analysis of the sample data points, the actual population mean should fall between these Lower and Upper Intervals for the Mean.

Median is the data point where 50% of all data points fall above this value and 50% below this value. Among the three first moment statistics, the median is least susceptible to outliers. A symmetrical distribution has the Median equal to the Arithmetic Mean. A skewed distribution exists when the Median is far away from the Mean. The Mode measures the most frequently occurring data point.

Minimum is the smallest value in the data set while Maximum is the largest value. Range is the difference between the Maximum and Minimum values.

The second moment measures a distribution's spread or width, and is frequently described using measures such as Standard Deviations, Variances, Quartiles, and Inter-

Quartile Ranges. Standard Deviation indicates the average deviation of all data points from their mean. It is a popular measure as is associated with risk (higher standard deviations mean a wider distribution, higher risk, or wider dispersion of data points around the mean) and its units are identical to original data set's. The Sample Standard Deviation differs from the Population Standard Deviation in that the former uses a degree of freedom correction to account for small sample sizes. Also, Lower and Upper Confidence Intervals are provided for the Standard Deviation and the true population standard deviation falls within this interval. If your data set covers every element of the population, use the Population Standard Deviation instead. The two Variance measures are simply the squared values of the standard deviations.

The Coefficient of Variability is the standard deviation of the sample divided by the sample mean, proving a unit-free measure of dispersion that can be compared across different distributions (you can now compare distributions of values denominated in millions of dollars with one in billions of dollars, or meters and kilograms, etc.). The First Quartile measures the 25th percentile of the data points when arranged from its smallest to largest value. The Third Quartile is the value of the 75th percentile data point. Sometimes quartiles are used as the upper and lower ranges of a distribution as it truncates the data set to ignore outliers. The Inter-Quartile Range is the difference between the third and first quartiles, and is often used to measure the width of the center of a distribution.

Skewness is the third moment in a distribution. Skewness characterizes the degree of asymmetry of a distribution around its mean. Positive skewness indicates a distribution with an asymmetric tail extending toward more positive values. Negative skewness indicates a distribution with an asymmetric tail extending toward more negative values.

Kurtosis characterizes the relative peakedness or flatness of a distribution compared to the normal distribution. It is the fourth moment in a distribution. A positive Kurtosis value indicates a relatively peaked distribution. A negative kurtosis indicates a relatively flat distribution. The Kurtosis measured here has been centered to zero (certain other kurtosis measures are centered around 3.0). While both are equally valid, centering across zero makes the interpretation simpler. A high positive Kurtosis indicates a peaked distribution around its center and leptokurtic or fat tails. This indicates a higher probability of extreme events (e.g., catastrophic events, terrorist attacks, stock market crashes) than is predicted in a normal distribution. Table 51 presents summary statistics.

Table 51. Summary Statistics.

Statistics	Time		
Observations	48.0000	Standard Deviation (Sample)	384.1219
Arithmetic Mean	923.7083	Standard Deviation (Population)	380.0995
Geometric Mean	851.8832	Lower Confidence Interval for Standard Deviation	329.1730
Trimmed Mean	897.7955	Upper Confidence Interval for Standard Deviation	463.5905

Standard Error of Arithmetic Mean	55.4432	Variance (Sample)	147549.6152
Lower Confidence Interval for Mean	812.8219	Variance (Population)	144475.6649
Upper Confidence Interval for Mean	1034.5948	Coefficient of Variability	0.4158
Median	842.0000	First Quartile (Q1)	600.0000
Minimum	390.0000	Third Quartile (Q3)	1209.0000
Maximum	2022.0000	Inter-Quartile Range	609.0000
Range	1632.0000	Skewness	0.9497
		Kurtosis	0.8407
Statistics	Accuracy		
Observations	48.0000	Standard Deviation (Sample)	0.4593
Arithmetic Mean	0.7083	Standard Deviation (Population)	0.4545
Geometric Mean	0.0000	Lower Confidence Interval for Standard Deviation	0.3936
Trimmed Mean	0.7273	Upper Confidence Interval for Standard Deviation	0.5544
Standard Error of Arithmetic Mean	0.0663	Variance (Sample)	0.2110
Lower Confidence Interval for Mean	0.5757	Variance (Population)	0.2066
Upper Confidence Interval for Mean	0.8409	Coefficient of Variability	0.6485
Median	1.0000	First Quartile (Q1)	0.0000
Minimum	0.0000	Third Quartile (Q3)	1.0000
Maximum	1.0000	Inter-Quartile Range	1.0000
Range	1.0000	Skewness	-0.9465
		Kurtosis	-1.1540
Statistics	Performance		
Observations	48.0000	Standard Deviation (Sample)	0.4583
Arithmetic Mean	1.2515	Standard Deviation (Population)	0.4535
Geometric Mean	1.1408	Lower Confidence Interval for Standard Deviation	0.3927
Trimmed Mean	1.2682	Upper Confidence Interval for Standard Deviation	0.5531
Standard Error of Arithmetic Mean	0.0661	Variance (Sample)	0.2100
Lower Confidence Interval for Mean	1.1192	Variance (Population)	0.2056
Upper Confidence Interval for Mean	1.3838	Coefficient of Variability	0.3662
Median	1.4216	First Quartile (Q1)	0.7463
Minimum	0.2977	Third Quartile (Q3)	1.6034
Maximum	1.8071	Inter-Quartile Range	0.8571
Range	1.5094	Skewness	-0.6754
		Kurtosis	-1.0138
Statistics	Confidence		
Observations	48.0000	Standard Deviation (Sample)	1.1910
Arithmetic Mean	7.1667	Standard Deviation (Population)	1.1785
Geometric Mean	7.0690	Lower Confidence Interval for Standard Deviation	1.0206
Trimmed Mean	7.1818	Upper Confidence Interval for Standard Deviation	1.4374
Standard Error of Arithmetic Mean	0.1719	Variance (Sample)	1.4184

Lower Confidence Interval for Mean	6.8229	Variance (Population)	1.3889
Upper Confidence Interval for Mean	7.5105	Coefficient of Variability	0.1662
Median	7.0000	First Quartile (Q1)	6.0000
Minimum	5.0000	Third Quartile (Q3)	8.0000
Maximum	9.0000	Inter-Quartile Range	2.0000
Range	4.0000	Skewness	0.1373
		Kurtosis	-0.8717
Statistics	InfoOvld		
Observations	48.0000	Standard Deviation (Sample)	1.1743
Arithmetic Mean	1.9375	Standard Deviation (Population)	1.1620
Geometric Mean	1.6591	Lower Confidence Interval for Standard Deviation	1.0063
Trimmed Mean	1.8409	Upper Confidence Interval for Standard Deviation	1.4172
Standard Error of Arithmetic Mean	0.1695	Variance (Sample)	1.3790
Lower Confidence Interval for Mean	1.5985	Variance (Population)	1.3503
Upper Confidence Interval for Mean	2.2765	Coefficient of Variability	0.6061
Median	2.0000	First Quartile (Q1)	1.0000
Minimum	1.0000	Third Quartile (Q3)	2.0000
Maximum	5.0000	Inter-Quartile Range	1.0000
Range	4.0000	Skewness	1.2773
		Kurtosis	0.9528

D. HETEROSKEDASTICITY, MICRONUMEROSITY, OUTLIERS AND NONLINEARITY

A common violation in forecasting and regression analysis is heteroskedasticity, that is, the variance of the errors increases over time. Visually, the width of the vertical data fluctuations increases or fans out over time, and typically, the coefficient of determination (R-squared coefficient) drops significantly when heteroskedasticity exists. If the variance of the dependent variable is not constant, then the error's variance will not be constant. Unless the heteroskedasticity of the dependent variable is pronounced, its effect will not be severe: the least-squares estimates will still be unbiased, and the estimates of the slope and intercept will either be normally distributed if the errors are normally distributed, or at least normally distributed asymptotically (as the number of data points becomes large) if the errors are not normally distributed. The estimate for the variance of the slope and overall variance will be inaccurate, but the inaccuracy is not likely to be substantial if the independent-variable values are symmetric about their mean.

If the number of data points is small (micronumerosity), it may be difficult to detect assumption violations. With small samples, assumption violations such as non-normality or heteroskedasticity of variances are difficult to detect even when they are present. With a small number of data points, linear regression offers less protection against violation of assumptions. With few data points, it may be hard to determine how well the fitted line

matches the data, or whether a nonlinear function would be more appropriate. Even if none of the test assumptions are violated, a linear regression on a small number of data points may not have sufficient power to detect a significant difference between the slope and zero, even if the slope is nonzero. The power depends on the residual error, the observed variation in the independent variable, the selected significance alpha level of the test, and the number of data points. Power decreases as the residual variance increases, decreases as the significance level is decreased (i.e., as the test is made more stringent), increases as the variation in observed independent variable increases, and increases as the number of data points increases.

Values may not be identically distributed because of the presence of outliers. Outliers are anomalous values in the data. Outliers may have a strong influence over the fitted slope and intercept, giving a poor fit to the bulk of the data points. Outliers tend to increase the estimate of residual variance, lowering the chance of rejecting the null hypothesis, i.e., creating higher prediction errors. They may be due to recording errors, which may be correctable, or they may be due to the dependent-variable values not all being sampled from the same population. Apparent outliers may also be due to the dependent-variable values being from the same, but non-normal, population. However, a point may be an unusual value in either an independent or dependent variable without necessarily being an outlier in the scatter plot. In regression analysis, the fitted line can be highly sensitive to outliers. In other words, least squares regression is not resistant to outliers, thus, neither is the fitted-slope estimate. A point vertically removed from the other points can cause the fitted line to pass close to it, instead of following the general linear trend of the rest of the data, especially if the point is relatively far horizontally from the center of the data.

Diagnostic Results

Variable	Heteroskedasticity		Micronumerosity		Outliers		Nonlinearity	
	W-Test	Hypothesis Test	Approximation	Natural Lower Bound	Natural Upper Bound	Number of Potential Outliers	Nonlinear Test	Hypothesis Test
	p-value	result	result				p-value	result
Y			no problems	168.91	1678.51	2		
Age	0.6898	Homoskedastic	no problems	14.86	61.01	3	0.6560	linear

E. AUTOCORRELATION OF THE DEPENDENT VARIABLE AND DISTRIBUTIVE LAGS OF THE INDEPENDENT VARIABLES

A typical issue when forecasting time-series data is whether the independent-variable values are truly independent of each other or are they dependent. Dependent variable values collected over a time-series may be autocorrelated. For serially correlated dependent-variable values, the estimates of the slope and intercept will be unbiased, but the estimates of their forecast and variances will not be reliable and hence the validity of certain statistical goodness-of-fit tests will be flawed. For instance, interest rates, inflation rates, sales, revenues, and many other time-series data are typically autocorrelated, where

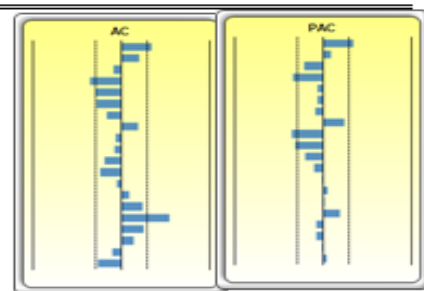
the value in the current period is related to the value in a previous period, and so forth (clearly, the inflation rate in March is related to February's level, which in turn, is related to January's level, and so forth). Ignoring such blatant relationships will yield biased and less accurate forecasts. In such events, an autocorrelated regression model or an ARIMA model may be better suited (Risk Simulator 1 Forecasting 1 ARIMA). Finally, the autocorrelation functions of a series that is nonstationary tend to decay slowly (see Nonstationary report).

If autocorrelation $AC(1)$ is nonzero, it means that the series is first order serially correlated. If $AC(k)$ dies off more or less geometrically with increasing lag, it implies that the series follows a low-order autoregressive process. If $AC(k)$ drops to zero after a small number of lags, it implies that the series follows a low-order moving-average process. Partial correlation $PAC(k)$ measures the correlation of values that are k periods apart after removing the correlation from the intervening lags. If the pattern of autocorrelation can be captured by an autoregression of order less than k , then the partial autocorrelation at lag k will be close to zero. Ljung-Box Q-statistics and their p-values at lag k has the null hypothesis that there is no autocorrelation up to order k . The dotted lines in the plots of the autocorrelations are the approximate two standard error bounds. If the autocorrelation is within these bounds, it is not significantly different from zero at the 5% significance level.

Autocorrelation measures the relationship to the past of the dependent Y variable to itself. Distributive Lags, in contrast, are time-lag relationships between the dependent Y variable and different independent X variables. For instance, the movement and direction of mortgage rates tend to follow the Federal Funds Rate but at a time lag (typically 1 to 3 months). Sometimes, time lags follow cycles and seasonality (e.g., ice cream sales tend to peak during the summer months and are hence related to last summer's sales, 12 months in the past). The distributive lag analysis below show how the dependent variable is related to each of the independent variables at various time lags, when all lags are considered simultaneously, to determine which time lags are statistically significant and should be considered.

Autocorrelation

Time Lag	AC	PAC	Lower Bound	Upper Bound	Q-Stat	Prob
1	0.3460	0.3460	-0.2887	0.2887	6.1119	0.0134
2	0.1993	0.0904	-0.2887	0.2887	8.1841	0.0167
3	-0.0894	-0.2100	-0.2887	0.2887	8.6102	0.0349
4	-0.3532	-0.3377	-0.2887	0.2887	15.4134	0.0039
5	-0.2969	-0.0665	-0.2887	0.2887	20.3338	0.0011
6	-0.2731	-0.0689	-0.2887	0.2887	24.5956	0.0004
7	-0.1603	-0.0919	-0.2887	0.2887	26.0995	0.0005
8	0.1936	0.2352	-0.2887	0.2887	28.3491	0.0004
9	-0.0646	-0.3595	-0.2887	0.2887	28.6057	0.0008
10	-0.0793	-0.3226	-0.2887	0.2887	29.0030	0.0012
11	-0.1845	-0.2028	-0.2887	0.2887	31.2119	0.0010
12	-0.2347	-0.1067	-0.2887	0.2887	34.8831	0.0005
13	-0.0465	-0.0134	-0.2887	0.2887	35.0312	0.0008
14	0.0836	0.0476	-0.2887	0.2887	35.5245	0.0012
15	0.2447	0.0159	-0.2887	0.2887	39.8806	0.0005
16	0.5420	0.1938	-0.2887	0.2887	61.9124	0.0000
17	0.2589	-0.0789	-0.2887	0.2887	67.1007	0.0000
18	0.1449	-0.0741	-0.2887	0.2887	68.7807	0.0000
19	-0.0953	-0.0143	-0.2887	0.2887	69.5324	0.0000
20	-0.2602	0.0431	-0.2887	0.2887	75.3335	0.0000



F. TEST FOR NORMALITY AND SPHERICITY OF ERRORS

Another requirement in running a regression model is the assumption of normality and sphericity of the error term. If the assumption of normality is violated or outliers are present, then the linear regression goodness-of-fit test may not be the most powerful or informative test available, and this could mean the difference between detecting a linear fit or not. If the errors are not independent and not normally distributed, it may indicate that the data might be autocorrelated or suffer from nonlinearities or other more destructive errors. Independence of the errors can also be detected in the heteroskedasticity tests (see Diagnostics report).

The Normality test on the errors performed is a nonparametric test, which makes no assumptions about the specific shape of the population from which the sample is drawn, allowing for smaller sample data sets to be analyzed. This test evaluates the null hypothesis of whether the sample errors were drawn from a normally distributed population, versus an alternate hypothesis that the data sample is not normally distributed. If the calculated D-Statistic is greater than or equal to the D-Critical values at various significance values then reject the null hypothesis and accept the alternate hypothesis (the errors are not normally distributed). Otherwise, if the D-Statistic is less than the D-Critical value, do not reject the null hypothesis (the errors are normally distributed). This test relies on two cumulative frequencies: one derived from the sample data set, the second from a theoretical distribution based on the mean and standard deviation of the sample data.

Test Result						
		Errors	Relative Frequency	Observed	Expected	O-E
Regression Error Average	0.00					
Standard Deviation of Errors	383.32	-514.60	0.02	0.02	0.0897	-0.0689
D Statistic	0.1125	-498.01	0.02	0.04	0.0969	-0.0553
D Critical at 1%	0.1162	-459.79	0.02	0.06	0.1152	-0.0527
D Critical at 5%	0.1250	-455.68	0.02	0.08	0.1173	-0.0339
D Critical at 10%	0.1488	-439.90	0.02	0.10	0.1256	-0.0214
Null Hypothesis: The errors are normally distributed.		-424.55	0.02	0.13	0.1340	-0.0090
		-416.90	0.02	0.15	0.1384	0.0074
Conclusion: The errors are normally distributed at the 1% alpha level.		-397.20	0.02	0.17	0.1501	0.0166
		-345.58	0.02	0.19	0.1837	0.0038
		-344.82	0.02	0.21	0.1842	0.0242
		-344.66	0.02	0.23	0.1843	0.0449
		-320.87	0.02	0.25	0.2013	0.0487
		-293.42	0.02	0.27	0.2220	0.0488
		-266.01	0.02	0.29	0.2439	0.0478
		-242.20	0.02	0.31	0.2637	0.0488
		-204.12	0.02	0.33	0.2972	0.0361
		-199.31	0.02	0.35	0.3016	0.0526
		-189.77	0.02	0.38	0.3103	0.0647
		-162.90	0.02	0.40	0.3354	0.0604

-153.71	0.02	0.42	0.3442	0.0725
-140.55	0.02	0.44	0.3569	0.0806
-137.01	0.02	0.46	0.3604	0.0979
-122.01	0.02	0.48	0.3751	0.1040
-81.79	0.02	0.50	0.4155	0.0845
-66.36	0.02	0.52	0.4313	0.0896
-65.33	0.02	0.54	0.4323	0.1093
-32.88	0.02	0.56	0.4658	0.0967
-11.55	0.02	0.58	0.4880	0.0954
-7.98	0.02	0.60	0.4917	0.1125
27.34	0.02	0.63	0.5284	0.0966
71.99	0.02	0.65	0.5745	0.0713
118.88	0.02	0.67	0.6218	0.0449
177.99	0.02	0.69	0.6788	0.0087
193.99	0.02	0.71	0.6936	0.0147
197.99	0.02	0.73	0.6973	0.0319
272.78	0.02	0.75	0.7616	-0.0116
281.23	0.02	0.77	0.7684	0.0024
296.67	0.02	0.79	0.7805	0.0112
338.53	0.02	0.81	0.8114	0.0011
373.32	0.02	0.83	0.8349	-0.0016
382.10	0.02	0.85	0.8406	0.0136
392.21	0.02	0.88	0.8469	0.0281
417.85	0.02	0.90	0.8622	0.0337
421.23	0.02	0.92	0.8641	0.0526
525.94	0.02	0.94	0.9150	0.0225
696.10	0.02	0.96	0.9653	-0.0070
1067.53	0.02	0.98	0.9973	-0.0182
1085.78	0.02	1.00	0.9977	0.0023

G. NONSTATIONARY ANALYSIS OF DEPENDENT VARIABLE

Sometimes, certain types of time-series data cannot be modeled using any other methods except for a stochastic process, because the underlying events are stochastic in nature. For instance, you cannot adequately model and forecast stock prices, interest rates, price of oil, and other commodity prices using a simple regression model, because these variables are highly uncertain and volatile, and does not follow a predefined static rule of behavior, in other words, the process is not stationary. Stationarity is checked here using the Runs Test while another visual clue is found in the Autocorrelation report (the ACF tends to decay slowly). A stochastic process is a sequence of events or paths generated by probabilistic laws. That is, random events can occur over time but are governed by specific statistical and probabilistic rules. The main stochastic processes include Random Walk or Brownian Motion, Mean-Reversion, and Jump-Diffusion. These processes can be used to forecast a multitude of variables that seemingly follow random trends but restricted by probabilistic laws. The process-generating equation is known in advance but the actual results generated is unknown.

The Random Walk Brownian Motion process can be used to forecast stock prices, prices of commodities, and other stochastic time-series data given a drift or growth rate and a

volatility around the drift path. The Mean-Reversion process can be used to reduce the fluctuations of the Random Walk process by allowing the path to target a long-term value, making it useful for forecasting time-series variables that have a long-term rate such as interest rates and inflation rates (these are long-term target rates by regulatory authorities or the market). The Jump-Diffusion process is useful for forecasting time-series data when the variable can occasionally exhibit random jumps, such as oil prices or price of electricity (discrete exogenous event shocks can make prices jump up or down). These processes can also be mixed and matched as required.

Statistical Summary

The following are the estimated parameters for a stochastic process given the data provided. It is up to you to determine if the probability of fit (similar to a goodness-of-fit computation) is sufficient to warrant the use of a stochastic process forecast, and if so, whether it is a random walk, mean-reversion, or a jump-diffusion model, or combinations thereof. In choosing the right stochastic process model, you will have to rely on past experiences and *a priori* economic and financial expectations of what the underlying data set is best represented by. These parameters can be entered into a stochastic process forecast (**Risk Simulator | Forecasting | Stochastic Processes**).

Periodic

Drift		Reversion		Jump	
Rate	1.10%	Rate	104.41%	Rate	14.89%
Volatility	43.91%	Long-Term		Jump	
		Value	933.20	Size	440.44

Probability of stochastic model fit: 30.58%
A high fit means a stochastic model is better than conventional models.

Runs	18	Standard Normal	-2.1106
Positive	24	P-Value (1-tail)	0.0174
Negative	24	P-Value (2-tail)	0.0348
Expected			
Run	25		

A low p-value (below 0.10, 0.05, 0.01) means that the sequence is not random and hence suffers from stationarity problems, and an ARIMA model might be more appropriate. Conversely, higher p-values indicate randomness and stochastic process models might be appropriate.

H. RESEARCH QUESTION ANALYSES

Q1: Does teamwork and ignorance interactively affect ITA performance?

Tests of Between-Subjects Effects

Dependent Variable: Performance

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	.122 ^a	3	.041	.183	.907
Intercept	75.181	1	75.181	339.294	.000
Teamwork	.047	1	.047	.213	.647
Ignorance	.066	1	.066	.298	.588
Teamwork * Ignorance	.008	1	.008	.038	.847
Error	9.749	44	.222		
Total	85.052	48			
Corrected Total	9.871	47			

a. R Squared = .012 (Adjusted R Squared = -.055)

Q2: Does teamwork affect ITA performance?

Independent variable: Time

Regression Statistics	
R-Squared (Coefficient of Determination)	0.0048
Adjusted R-Squared	0.0000
Multiple R (Multiple Correlation Coefficient)	0.0691
Standard Error of the Estimates (SEy)	0.4621
Number of Observations	48

The R-Squared or Coefficient of Determination indicates that 0.00 of the variation in the dependent variable can be explained and accounted for by the independent variables in this regression analysis. However, in a multiple regression, the Adjusted R-Squared takes into account the existence of additional independent variables or regressors and adjusts this R-Squared value to a more accurate view of the regression's explanatory power. Hence, only 0.00 of the variation in the dependent variable can be explained by the regressors.

The Multiple Correlation Coefficient (Multiple R) measures the correlation between the actual dependent variable (Y) and the estimated or fitted (Y) based on the regression equation. This is also the square root of the Coefficient of Determination (R-Squared).

The Standard Error of the Estimates (SEy) describes the dispersion of data points above and below the regression line or plane. This value is used as part of the calculation to obtain the confidence interval of the estimates later.

Regression Results		
	Intercept	Teamwork
Coefficients	1.2202	0.0626
Standard Error	0.0943	0.1334
t-Statistic	12.9350	0.4696
p-Value	0.0000	0.6409
Lower 5%	1.0303	-0.2059
Upper 95%	1.4101	0.3312

Degrees of Freedom	Hypothesis Test		
Degrees of Freedom for Regression	1	Critical t-Statistic (99% confidence with df of 46)	2.6870
Degrees of Freedom for Residual	46	Critical t-Statistic (95% confidence with df of 46)	2.0129
Total Degrees of Freedom	47	Critical t-Statistic (90% confidence with df of 46)	1.6787

The Coefficients provide the estimated regression intercept and slopes. For instance, the coefficients are estimates of the true; population b values in the following regression equation $Y = b_0 + b_1X_1 + b_2X_2 + \dots + b_nX_n$. The Standard Error measures how accurate the predicted Coefficients are, and the t-Statistics are the ratios of each predicted Coefficient to its Standard Error.

The t-Statistic is used in hypothesis testing, where we set the null hypothesis (H_0) such that the real mean of the Coefficient = 0, and the alternate hypothesis (H_a) such that the real mean of the Coefficient is not equal to 0. A t-test is performed and the calculated t-Statistic is compared to the critical values at the relevant Degrees of Freedom for Residual. The t-test is very important as it calculates if each of the coefficients is statistically significant in the presence of the other regressors. This means that the t-test statistically verifies whether a regressor or independent variable should remain in the regression or it should be dropped.

The Coefficient is statistically significant if its calculated t-Statistic exceeds the Critical t-Statistic at the relevant degrees of freedom (df). The three main confidence levels used to test for significance are 90%, 95% and 99%. If a Coefficient's t-Statistic exceeds the Critical level, it is considered statistically significant. Alternatively, the p-Value calculates each t-Statistic's probability of occurrence, which means that the smaller the p-Value, the more significant the Coefficient. The usual significant levels for the p-Value are 0.01, 0.05, and 0.10, corresponding to the 99%, 95%, and 90% confidence levels.

The Coefficients with their p-Values highlighted in blue indicate that they are statistically significant at the 90% confidence or 0.10 alpha level, while those highlighted in red indicate that they are not statistically significant at any other alpha levels.

Test Statistics^a

Performance	
Mann-Whitney U	265.000
Wilcoxon W	565.000
Z	-.474
Asymp. Sig. (2-tailed)	.635

a. Grouping Variable: Teamwork

Q3: Does ignorance affect ITA performance?

Test Statistics^a

Performance	
Mann-Whitney U	208.000
Wilcoxon W	508.000
Z	-1.650
Asymp. Sig. (2-tailed)	.099

a. Grouping Variable: Ignorance

Dependent variable: Performance

Regression Statistics

R-Squared (Coefficient of Determination)	0.0067
Adjusted R-Squared	0.0000
Multiple R (Multiple Correlation Coefficient)	0.0818
Standard Error of the Estimates (SEy)	0.4617
Number of Observations	48

Regression Results

	Intercept	Ignorance
Coefficients	1.2144	0.0742
Standard Error	0.0942	0.1333
t-Statistic	12.8861	0.5569
p-Value	0.0000	0.5803
Lower 5%	1.0247	-0.1940
Upper 95%	1.4041	0.3425

Q4: Does teamwork and ignorance interactively affect ITA time?

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	4603525.417 ^a	3	1534508.472	28.962	.000	.664
Intercept	40955380.080	1	40955380.080	772.973	.000	.946
Teamwork	1722176.333	1	1722176.333	32.504	.000	.425
Ignorance	2847002.083	1	2847002.083	53.733	.000	.550
Teamwork * Ignorance	34347.000	1	34347.000	.648	.425	.015
Error	2331306.500	44	52984.239			
Total	47890212.000	48				
Corrected Total	6934831.917	47				

Q5: Does teamwork affect ITA time?

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	1722176.333 ^a	1	1722176.333	15.198	.000	.248
Intercept	40955380.080	1	40955380.080	361.418	.000	.887
Teamwork	1722176.333	1	1722176.333	15.198	.000	.248
Error	5212655.583	46	113318.600			
Total	47890212.000	48				
Corrected Total	6934831.917	47				

Regression Statistics

R-Squared (Coefficient of Determination)	0.2483
Adjusted R-Squared	0.2320
Multiple R (Multiple Correlation Coefficient)	0.4983
Standard Error of the Estimates (SEy)	336.6283
Number of Observations	48

Dependent variable: Time

Regression Results

	Intercept	Teamwork
Coefficients	734.2917	378.8333
Standard Error	68.7140	97.1762
t-Statistic	10.6862	3.8984
p-Value	0.0000	0.0003
Lower 5%	595.9776	183.2278
Upper 95%	872.6057	574.4389

Test Statistics^a

	Time
Mann-Whitney U	120.000
Wilcoxon W	420.000
Z	-3.464
Asymp. Sig. (2-tailed)	.001

a. Grouping Variable: Teamwork

Q6: Does ignorance affect ITA time?

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	2847002.083 ^a	1	2847002.083	32.037	.000	.411
Intercept	40955380.080	1	40955380.080	460.867	.000	.909
Ignorance	2847002.083	1	2847002.083	32.037	.000	.411
Error	4087829.833	46	88865.866			
Total	47890212.000	48				
Corrected Total	6934831.917	47				

Regression Statistics

R-Squared (Coefficient of Determination)	0.4105
Adjusted R-Squared	0.3977
Multiple R (Multiple Correlation Coefficient)	0.6407
Standard Error of the Estimates (SEy)	298.1038
Number of Observations	48

Dependent variable: Time

Regression Results

	Intercept	Ignorance
Coefficients	1167.2500	-487.0833
Standard Error	60.8502	86.0551
t-Statistic	19.1824	-5.6601
p-Value	0.0000	0.0000
Lower 5%	1044.7649	-660.3034
Upper 95%	1289.7351	-313.8633

Test Statistics^a

	Time
Mann-Whitney U	60.000
Wilcoxon W	360.000
Z	-4.701
Asymp. Sig. (2-tailed)	.000

a. Grouping Variable: Ignorance

Q7: Does teamwork and ignorance interactively affect ITA accuracy?

Tests of Between-Subjects Effects

Dependent Variable: Accuracy

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	1.083 ^a	3	.361	1.799	.161
Intercept	24.083	1	24.083	119.962	.000
Teamwork	.750	1	.750	3.736	.060
Ignorance	.333	1	.333	1.660	.204
Teamwork * Ignorance	.000	1	.000	.000	1.000
Error	8.833	44	.201		
Total	34.000	48			
Corrected Total	9.917	47			

a. R Squared = .109 (Adjusted R Squared = .049)

Q8: Does teamwork affect ITA accuracy?

Dependent variable: Accuracy

Regression Results				
Log Likelihood Value	-27.1141	Approach	Logit	
Variable	Coefficients	Standard Error	Z-Statistic	p-Value
	0.3367	0.4140	0.8133	0.4161
Teamwork	1.2726	0.6866	1.8535	0.0638

Limited Dependent Variables describe the situation where the dependent variable contains data that are limited in scope and range, such as binary responses (0 or 1), truncated, ordered, or censored data. For instance, given a set of independent variables (e.g., age, income, education level of credit card or mortgage loan holders), we can model the probability of default using maximum likelihood estimation (MLE). The response or dependent variable Y is binary, that is, it can have only two possible outcomes which we will denote as 1 and 0 (e.g., Y may represent presence/absence of a certain condition,

defaulted/not defaulted on previous loans, success/failure of some device, answer yes/no on a survey, etc.) and we also have a vector of independent variable regressors X , which are assumed to influence the outcome Y . A typical ordinary least squares regression approach is invalid because the regression errors are heteroskedastic and non-normal, and the resulting estimated probability estimates will return nonsensical values of above 1 or below 0. MLE analysis handles these problems using an iterative optimization routine to maximize a log likelihood function when the dependent variables are limited.

A Logit or Logistic regression is used for predicting the probability of occurrence of an event by fitting data to a logistic curve. It is a generalized linear model used for binomial regression, and like many forms of regression analysis, it makes use of several predictor variables that may be either numerical or categorical. MLE applied in a binary multivariate logistic analysis is used to model dependent variables to determine the expected probability of success of belonging to a certain group. The estimated coefficients for the Logit model are the logarithmic odds ratios, and cannot be interpreted directly as probabilities. A quick computation is first required and the approach is simple.

Specifically, the Logit model is specified as Estimated $Y = \text{LN}[P_i/(1-P_i)]$ or conversely, $P_i = \text{EXP}(\text{Estimated } Y)/(1+\text{EXP}(\text{Estimated } Y))$, and the coefficients β_i are the log odds ratios, so taking the antilog or $\text{EXP}(\beta_i)$ we obtain the odds ratio of $P_i/(1-P_i)$. This means that with an increase in a unit of β_i the log odds ratio increases by this amount. Finally, the rate of change in the probability $dP/dX = \beta_i P_i(1-P_i)$. The Standard Error measures how accurate the predicted Coefficients are, and the t-Statistics are the ratios of each predicted Coefficient to its Standard Error and are used in the typical regression hypothesis test of the significance of each estimated parameter. To estimate the probability of success of belonging to a certain group (e.g., predicting if a smoker will develop chest complications given the amount smoked per year), simply compute the Estimated Y value using the MLE coefficients. For example, if the model is $Y = 1.1 + 0.005$ (Cigarettes) then for someone smoking 100 packs per year has an Estimated Y of $1.1 + 0.005(100) = 1.6$. Next, compute the inverse antilog of the odds ratio by doing: $\text{EXP}(\text{Estimated } Y)/[1 + \text{EXP}(\text{Estimated } Y)] = \text{EXP}(1.6)/(1 + \text{EXP}(1.6)) = 0.8320$. So, such a person has an 83.20% chance of developing some chest complications in his lifetime.

A Probit model (sometimes also known as a Normit model) is a popular alternative specification for a binary response model which employs a probit function estimated using maximum likelihood estimation and the approach is called probit regression. The Probit and Logistic regression models tend to produce very similar predictions where the parameter estimates in a logistic regression tend to be 1.6 to 1.8 times higher than they are in a corresponding Probit model. The choice of using a Probit or Logit is entirely up to convenience, and the main distinction is that the logistic distribution has a higher kurtosis (fatter tails) to account for extreme values. For example, suppose that house ownership is the decision to be modeled, and this response variable is binary (home purchase or no home purchase) and depends on a series of independent variables X_i such as income, age, and so forth, such that $I_i = \beta_0 + \beta_1 X_1 + \dots + \beta_n X_n$, where the larger the

value of I_i , the higher the probability of home ownership. For each family, a critical I^* threshold exists, where if exceeded, the house is purchased, otherwise, no home is purchased, and the outcome probability (P) is assumed to be normally distributed, such that $P_i = \text{CDF}(I)$ using a standard normal cumulative distribution function (CDF). Therefore, use the estimated coefficients exactly like that of a regression model and using the Estimated Y value, apply a standard normal distribution (you can use Excel's NORMSDIST function or Risk Simulator's Distributional Analysis tool by selecting Normal distribution and setting the mean to be 0 and standard deviation to be 1). Finally, to obtain a Probit or probability unit measure, set $I_i + 5$ (this is because whenever the probability $P_i < 0.5$, the estimated I_i is negative, due to the fact that the normal distribution is symmetrical around a mean of zero).

The Tobit Model (Censored Tobit) is an econometric and biometric modeling method used to describe the relationship between a non-negative dependent variable Y_i and one or more independent variables X_i . A Tobit model is an econometric model in which the dependent variable is censored; that is, the dependent variable is censored because values below zero are not observed. The Tobit model assumes that there is a latent unobservable variable Y^* . This variable is linearly dependent on the X_i variables via a vector of β_i coefficients that determine their inter-relationships. In addition, there is a normally distributed error term U_i to capture random influences on this relationship. The observable variable Y_i is defined to be equal to the latent variables whenever the latent variables are above zero and Y_i is assumed to be zero otherwise. That is, $Y_i = Y^*$ if $Y^* > 0$ and $Y_i = 0$ if $Y^* = 0$. If the relationship parameter β_i is estimated by using ordinary least squares regression of the observed Y_i on X_i , the resulting regression estimators are inconsistent and yield downward biased slope coefficients and an upward biased intercept. Only MLE would be consistent for a Tobit model. In the Tobit model, there is an ancillary statistic called sigma, which is equivalent to the standard error of estimate in a standard ordinary least squares regression and the estimated coefficients are used the same way as a regression analysis.

Chi-Square Tests

	Value	df	Asymptotic Significance (2- sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)
Pearson Chi-Square	3.630 ^a	1	.057		
Continuity Correction ^b	2.521	1	.112		
Likelihood Ratio	3.721	1	.054		
Fisher's Exact Test				.111	.055
Linear-by-Linear Association	3.555	1	.059		
N of Valid Cases	48				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 7.00.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	.275	.057
	Cramer's V	.275	.057
N of Valid Cases		48	

Q9: Does ignorance affect ITA accuracy?

Dependent variable: Accuracy

Results

Log Likelihood Value	-28.1593	Approach	Logit	
Variable	Coefficients	Standard Error	Z-Statistic	p-Value
	1.3325	0.5023	2.6530	0.0080
Ignorance	-0.8222	0.6558	-1.2538	0.2099

Variables: Accuracy * Ignorance

Chi-Square Tests

	Value	df	Asymptotic Significance (2- sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)
Pearson Chi-Square	1.613 ^a	1	.204		
Continuity Correction ^b	.908	1	.341		
Likelihood Ratio	1.631	1	.202		
Fisher's Exact Test				.341	.171
Linear-by-Linear Association	1.580	1	.209		
N of Valid Cases	48				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 7.00.

b. Computed only for a 2x2 table

Q10: Does teamwork and ignorance interact with ITA confidence?

Tests of Between-Subjects Effects

Dependent Variable: Confidence

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	4.167 ^a	3	1.389	.978	.412
Intercept	2465.333	1	2465.333	1735.595	.000
Teamwork	.750	1	.750	.528	.471

Ignorance	1.333	1	1.333	.939	.338
Teamwork * Ignorance	2.083	1	2.083	1.467	.232
Error	62.500	44	1.420		
Total	2532.000	48			
Corrected Total	66.667	47			

a. R Squared = .063 (Adjusted R Squared = -.001)

Q11: Does teamwork affect ITA confidence?

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	.750 ^a	1	.750	.523	.473	.011
Intercept	2465.333	1	2465.333	1720.435	.000	.974
Teamwork	.750	1	.750	.523	.473	.011
Error	65.917	46	1.433			
Total	2532.000	48				
Corrected Total	66.667	47				

a. R Squared = .011 (Adjusted R Squared = -.010)

b. Computed using alpha = .05

Dependent variable: Confidence

Regression Results

	Intercept	Teamwork
Coefficients	7.2917	-0.2500
Standard Error	0.2444	0.3456
t-Statistic	29.8410	-0.7235
p-Value	0.0000	0.4731
Lower 5%	6.7998	-0.9456
Upper 95%	7.7835	0.4456

Test Statistics^a

	Confidence
Mann-Whitney U	253.000
Wilcoxon W	553.000
Z	-.746
Asymp. Sig. (2-tailed)	.456

a. Grouping Variable: Teamwork

Q12: Does ignorance affect ITA confidence?

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	1.333 ^a	1	1.333	.939	.338	.020
Intercept	2465.333	1	2465.333	1735.796	.000	.974
Ignorance	1.333	1	1.333	.939	.338	.020
Error	65.333	46	1.420			
Total	2532.000	48				
Corrected Total	66.667	47				

a. R Squared = .020 (Adjusted R Squared = -.001)

b. Computed using alpha = .05

Dependent Variable: Confidence

Regression Results

	Intercept	Ignorance
Coefficients	7.3333	-0.3333
Standard Error	0.2433	0.3440
t-Statistic	30.1452	-0.9689
p-Value	0.0000	0.3377
Lower 5%	6.8437	-1.0258
Upper 95%	7.8230	0.3592

Test Statistics^a

	Confidence
Mann-Whitney U	247.500
Wilcoxon W	547.500
Z	-.863
Asymp. Sig. (2-tailed)	.388

a. Grouping Variable: Ignorance

Q13: Does teamwork and ignorance interactively affect perceptions of information overload?

ANOVA without simulated data:

Tests of Between-Subjects Effects

Dependent Variable: InfoOvld

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power ^b
Corrected Model	6.563 ^a	3	2.188	1.652	.191	.101	4.957	.403
Intercept	180.188	1	180.188	136.107	.000	.756	136.107	1.000
Teamwork	.188	1	.188	.142	.708	.003	.142	.066
Ignorance	1.688	1	1.688	1.275	.265	.028	1.275	.197
Teamwork * Ignorance	4.688	1	4.688	3.541	.067	.074	3.541	.453
Error	58.250	44	1.324					
Total	245.000	48						
Corrected Total	64.813	47						

a. R Squared = .101 (Adjusted R Squared = .040)

b. Computed using alpha = .05

ANOVA with simulated data:

Tests of Between-Subjects Effects

Dependent Variable: InfoOvld

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power ^b
Corrected Model	52.098 ^a	3	17.366	13.324	.000	.083	39.973	1.000
Intercept	1643.223	1	1643.223	1260.788	.000	.740	1260.788	1.000
Teamwork	1.080	1	1.080	.829	.363	.002	.829	.149
Ignorance	10.938	1	10.938	8.392	.004	.019	8.392	.824
Teamwork * Ignorance	40.080	1	40.080	30.752	.000	.065	30.752	1.000
Error	578.679	444	1.303					
Total	2274.000	448						
Corrected Total	630.777	447						

a. R Squared = .083 (Adjusted R Squared = .076)

b. Computed using alpha = .05

Q14: Does teamwork affect perceptions of information overload?

Dependent variable: InfoOvld

Regression Results		
	Intercept	Teamwork
Coefficients	2.0000	-0.1250
Standard Error	0.2419	0.3422
t-Statistic	8.2664	-0.3653
p-Value	0.0000	0.7165
Lower 5%	1.5130	-0.8137
Upper 95%	2.4870	0.5637

Test Statistics^a

	InfoOvld
Mann-Whitney U	284.500
Wilcoxon W	584.500
Z	-.078
Asymp. Sig. (2-tailed)	.938

a. Grouping Variable: Teamwork

Q15: Does ignorance affect perceptions of information overload?

Dependent Variable: InfoOvld

Regression Results		
	Intercept	Ignorance
Coefficients	2.1250	-0.3750
Standard Error	0.2391	0.3382
t-Statistic	8.8867	-1.1089
p-Value	0.0000	0.2732
Lower 5%	1.6437	-1.0557
Upper 95%	2.6063	0.3057

Test Statistics^a

	InfoOvld
Mann-Whitney U	251.000
Wilcoxon W	551.000
Z	-.819
Asymp. Sig. (2-tailed)	.413

a. Grouping Variable: Ignorance

Q16: Does ignorance affect perceptions of social impact?

Tests of Between-Subjects Effects

Dependent Variable: Soclmpact

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	2.667 ^a	1	2.667	2.588	.122
Intercept	80.667	1	80.667	78.294	.000
Ignorance	2.667	1	2.667	2.588	.122
Error	22.667	22	1.030		
Total	106.000	24			
Corrected Total	25.333	23			

a. R Squared = .105 (Adjusted R Squared = .065)

Test Statistics^a

Soclmpact	
Mann-Whitney U	52.000
Wilcoxon W	130.000
Z	-1.253
Asymp. Sig. (2-tailed)	.210
Exact Sig. [2*(1-tailed Sig.)]	.266 ^b

a. Grouping Variable: Ignorance

b. Not corrected for ties.

Q17: Does any scenario affect ITA time?

Tests of Between-Subjects Effects

Dependent Variable: Time

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	548592.083 ^a	3	182864.028	1.260	.300
Intercept	40955380.080	1	40955380.080	282.175	.000
Scenario	548592.083	3	182864.028	1.260	.300
Error	6386239.833	44	145141.814		
Total	47890212.000	48			
Corrected Total	6934831.917	47			

a. R Squared = .079 (Adjusted R Squared = .016)

Regression Statistics	
R-Squared (Coefficient of Determination)	0.0737
Adjusted R-Squared	0.0535
Multiple R (Multiple Correlation Coefficient)	0.2714
Standard Error of the Estimates (SEy)	373.7019
Number of Observations	48

Regression Results		
	Intercept	Scenario
Coefficients	693.0417	92.2667
Standard Error	132.1236	48.2447
t-Statistic	5.2454	1.9125
p-Value	0.0000	0.0621
Lower 5%	427.0907	-4.8449
Upper 95%	958.9926	189.3782

Test Statistics^{a,b}

Time	
Chi-Square	2.342
df	3
Asymp. Sig.	.505

a. Kruskal Wallis Test

b. Grouping Variable:
Scenario

Q18: Does scenario outcome affect ITA time?

Tests of Between-Subjects Effects

Dependent Variable: Time

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	206981.333 ^a	1	206981.333	1.415	.240
Intercept	40955380.080	1	40955380.080	280.022	.000
Outcome	206981.333	1	206981.333	1.415	.240
Error	6727850.583	46	146257.621		
Total	47890212.000	48			
Corrected Total	6934831.917	47			

a. R Squared = .030 (Adjusted R Squared = .009)

Dependent variable: Time

Regression Results		
	Intercept	Outcome
Coefficients	858.0417	131.3333
Standard Error	78.0645	110.3999
t-Statistic	10.9914	1.1896
p-Value	0.0000	0.2403
Lower 5%	700.9060	-90.8901
Upper 95%	1015.1774	353.5568

Test Statistics^a

	Time
Mann-Whitney U	248.000
Wilcoxon W	548.000
Z	-.825
Asymp. Sig. (2-tailed)	.409

a. Grouping Variable: Outcome

Q19: Does any scenario affect ITA performance?

Tests of Between-Subjects Effects

Dependent Variable: Performance

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	1.557 ^a	3	.519	2.747	.054
Intercept	75.181	1	75.181	397.885	.000
Scenario	1.557	3	.519	2.747	.054
Error	8.314	44	.189		
Total	85.052	48			
Corrected Total	9.871	47			

a. R Squared = .158 (Adjusted R Squared = .100)

Test Statistics^{a,b}

	Performance
Chi-Square	6.975
df	3
Asymp. Sig.	.073

a. Kruskal Wallis Test

b. Grouping Variable: Scenario

Dependent variable: Performance

Regression Results		
	Intercept	Scenario
Coefficients	1.4072	-0.0623
Standard Error	0.1618	0.0591
t-Statistic	8.6955	-1.0542
p-Value	0.0000	0.2973
Lower 5%	1.0815	-0.1812
Upper 95%	1.7330	0.0567

Q20: Does scenario outcome affect ITA performance?

Tests of Between-Subjects Effects

Dependent Variable: Performance

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	.411 ^a	1	.411	1.998	.164
Intercept	75.181	1	75.181	365.565	.000
Outcome	.411	1	.411	1.998	.164
Error	9.460	46	.206		
Total	85.052	48			
Corrected Total	9.871	47			

a. R Squared = .042 (Adjusted R Squared = .021)

Regression Results		
	Intercept	Scenario Type
Coefficients	1.1590	0.1850
Standard Error	0.0926	0.1309
t-Statistic	12.5202	1.4135
p-Value	0.0000	0.1642
Lower 5%	0.9726	-0.0785
Upper 95%	1.3453	0.4486

Test Statistics^a

	Performance
Mann-Whitney U	221.000
Wilcoxon W	521.000
Z	-1.382
Asymp. Sig. (2-tailed)	.167

a. Grouping Variable: Outcome

Q21: Does any scenario affect ITA accuracy?

Dependent variable: Accuracy

Results

Log Likelihood	Value	-28.9343		Approach	Logit
	Variable	Coefficients	Standard Error	Z-Statistic	p-Value
		1.0854	0.7896	1.3746	0.1692
	Scenario	-0.0791	0.2845	-0.2779	0.7811

Variables: Scenario * Accuracy

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.857 ^a	3	.077
Likelihood Ratio	10.072	3	.018
Linear-by-Linear Association	.079	1	.779
N of Valid Cases	48		

a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is 3.50.

Q22: Does scenario outcome affect ITA accuracy?

Dependent variable: Accuracy

Results

Log Likelihood Value	-27.1141	Approach	Logit	
Variable	Coefficients	Standard Error	Z-Statistic	p-Value
	0.3367	0.4140	0.8133	0.4161
Scenario Type	1.2726	0.6866	1.8535	0.0638

Variables: Outcome * Accuracy

Chi-Square Tests

	Value	df	Asymptotic Significance (2- sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)
Pearson Chi-Square	3.630 ^a	1	.057		
Continuity Correction ^b	2.521	1	.112		
Likelihood Ratio	3.721	1	.054		
Fisher's Exact Test				.111	.055
Linear-by-Linear Association	3.555	1	.059		
N of Valid Cases	48				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 7.00.

b. Computed only for a 2x2 table

Q23: Does any scenario affect ITA decision confidence?

Tests of Between-Subjects Effects

Dependent Variable: Confidence

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	18.833 ^a	3	6.278	5.775	.002
Intercept	2465.333	1	2465.333	2267.763	.000
Scenario	18.833	3	6.278	5.775	.002
Error	47.833	44	1.087		
Total	2532.000	48			
Corrected Total	66.667	47			

a. R Squared = .283 (Adjusted R Squared = .234)

Dependent variable: Confidence

Regression Statistics

R-Squared (Coefficient of Determination)	0.0563
Adjusted R-Squared	0.0357
Multiple R (Multiple Correlation Coefficient)	0.2372
Standard Error of the Estimates (SEy)	1.1695
Number of Observations	48

Regression Results

	Intercept	Scenario
Coefficients	6.5417	0.2500
Standard Error	0.4135	0.1510
t-Statistic	15.8208	1.6558
p-Value	0.0000	0.1046
Lower 5%	5.7094	-0.0539
Upper 95%	7.3740	0.5539

Test Statistics^{a,b}

	Confidence
Chi-Square	12.123
df	3
Asymp. Sig.	.007

a. Kruskal Wallis Test

b. Grouping Variable:
Scenario

Q24: Does scenario outcome affect ITA decision confidence?

Dependent variable: Confidence

Regression Statistics

R-Squared (Coefficient of Determination)	0.2813
Adjusted R-Squared	0.2656
Multiple R (Multiple Correlation Coefficient)	0.5303
Standard Error of the Estimates (SEy)	1.0206
Number of Observations	48

Regression Results

	Intercept	Outcome
Coefficients	6.5417	1.2500
Standard Error	0.2083	0.2946
t-Statistic	31.4000	4.2426
p-Value	0.0000	0.0001
Lower 5%	6.1223	0.6569
Upper 95%	6.9610	1.8431

Test Statistics^a

	Confidence
Mann-Whitney U	125.500
Wilcoxon W	425.500
Z	-3.463
Asymp. Sig. (2-tailed)	.001

a. Grouping Variable: Outcome

Tests of Between-Subjects Effects

Dependent Variable: Confidence

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power ^b
Corrected Model	18.750 ^a	1	18.750	18.000	.000	.281	18.000	.986
Intercept	2465.333	1	2465.333	2366.720	.000	.981	2366.720	1.000
Outcome	18.750	1	18.750	18.000	.000	.281	18.000	.986
Error	47.917	46	1.042					
Total	2532.000	48						
Corrected Total	66.667	47						

a. R Squared = .281 (Adjusted R Squared = .266)

b. Computed using alpha = .05

Q25: Does any scenario affect perceptions of information overload?

Tests of Between-Subjects Effects

Dependent Variable: InfoOvld

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	1.563 ^a	3	.521	.362	.781
Intercept	180.188	1	180.188	125.348	.000
Scenario	1.563	3	.521	.362	.781
Error	63.250	44	1.438		
Total	245.000	48			
Corrected Total	64.813	47			

a. R Squared = .024 (Adjusted R Squared = -.042)

Dependent variable: InfoOvld

Regression Results		
	Intercept	Scenario
Coefficients	1.8333	0.0417
Standard Error	0.4193	0.1531
t-Statistic	4.3721	0.2721
p-Value	0.0001	0.7867
Lower 5%	0.9893	-0.2665
Upper 95%	2.6774	0.3499

Test Statistics^{a,b}

InfoOvld	
Chi-Square	1.412
Df	3
Asymp. Sig.	.703

a. Kruskal Wallis Test

b. Grouping Variable:
Scenario

Q26: Does scenario outcome affect perceptions of information overload?

Tests of Between-Subjects Effects

Dependent Variable: InfoOvld

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	.521 ^a	1	.521	.373	.545
Intercept	180.188	1	180.188	128.922	.000
Outcome	.521	1	.521	.373	.545
Error	64.292	46	1.398		
Total	245.000	48			
Corrected Total	64.813	47			

a. R Squared = .008 (Adjusted R Squared = -.014)

Dependent variable: InfoOvld

Regression Results		
	Intercept	Outcome
Coefficients	2.0417	-0.2083
Standard Error	0.2413	0.3413
t-Statistic	8.4604	-0.6105
p-Value	0.0000	0.5446
Lower 5%	1.5559	-0.8953
Upper 95%	2.5274	0.4786

Test Statistics^a

	InfoOvld
Mann-Whitney U	257.500
Wilcoxon W	557.500
Z	-.675
Asymp. Sig. (2-tailed)	.499

a. Grouping Variable: Outcome

Q27—30: Does age, gender, education, experience, affect ITA time?

Dependent variable: Time

Regression Statistics

R-Squared (Coefficient of Determination)	0.0575
Adjusted R-Squared	0.0000
Multiple R (Multiple Correlation Coefficient)	0.2399
Standard Error of the Estimates (SEy)	389.8682
Number of Observations	48

Regression Results

	Intercept	Age	Gender	Education	Experience
Coefficients	888.2464	1.3545	165.0673	-94.9429	-1.2336
Standard Error	242.8952	6.0320	141.9960	104.3249	10.3233
t-Statistic	3.6569	0.2246	1.1625	-0.9101	-0.1195
p-Value	0.0007	0.8234	0.2515	0.3679	0.9054
Lower 5%	398.4015	-10.8102	-121.2949	-305.3340	-22.0525
Upper 95%	1378.0913	13.5192	451.4295	115.4483	19.5852

Q31—34: Does age, gender, education, experience, affect ITA accuracy?

Dependent variable: Accuracy

Regression Results

Log Likelihood Value	-25.5846	Approach	Logit	
Variable	Coefficients	Standard Error	Z-Statistic	p-Value
	0.4870	1.3146	0.3704	0.7111
Age	-0.0557	0.0358	-1.5542	0.1201
Gender	1.3960	0.7897	1.7678	0.0771
Education	1.0282	0.6753	1.5227	0.1278
Experience	-0.0241	0.0679	-0.3551	0.7225

Q32: Does gender affect ITA accuracy?

Dependent variable: Accuracy

Results

Log Likelihood Value	-27.7332	Approach	Logit		
Variable	Coefficients	Standard Error	Z-Statistic	p-Value	
	0.0018	0.6325	0.0029	0.9977	
Gender	1.1673	0.7386	1.5805	0.1140	

Q35—38: Does age, gender, education, experience affect ITA performance?

Dependent variable: Performance

Regression Statistics

R-Squared (Coefficient of Determination)	0.1358
Adjusted R-Squared	0.0554
Multiple R (Multiple Correlation Coefficient)	0.3685
Standard Error of the Estimates (SEy)	0.4454
Number of Observations	48

Regression Results

	Intercept	Age	Gender	Education	Experience
Coefficients	1.1661	-0.0115	0.2089	0.2403	-0.0049
Standard Error	0.2775	0.0069	0.1622	0.1192	0.0118
t-Statistic	4.2023	-1.6700	1.2877	2.0161	-0.4188
p-Value	0.0001	0.1022	0.2047	0.0501	0.6775
Lower 5%	0.6065	-0.0254	-0.1183	-0.0001	-0.0287
Upper 95%	1.7258	0.0024	0.5361	0.4806	0.0188

Q37: Does education affect ITA performance?

Dependent variable: Performance

Regression Results

	Intercept	Education
Coefficients	1.0802	0.1126
Standard Error	0.1690	0.1023
t-Statistic	6.3918	1.1011
p-Value	0.0000	0.2766
Lower 5%	0.7400	-0.0933
Upper 95%	1.4204	0.3186

Q39—42: Does age, gender, education, experience affect ITA confidence?

Dependent variable: Confidence

Regression Statistics	
R-Squared (Coefficient of Determination)	0.1359
Adjusted R-Squared	0.0555
Multiple R (Multiple Correlation Coefficient)	0.3686
Standard Error of the Estimates (SEy)	1.1575
Number of Observations	48

Regression Results					
	Intercept	Age	Gender	Education	Experience
Coefficients	6.5898	-0.0167	0.0153	0.7489	0.0322
Standard Error	0.7211	0.0179	0.4216	0.3097	0.0306
t-Statistic	9.1383	-0.9299	0.0362	2.4179	1.0492
p-Value	0.0000	0.3576	0.9713	0.0199	0.3000
Lower 5%	5.1355	-0.0528	-0.8349	0.1243	-0.0297
Upper 95%	8.0441	0.0195	0.8654	1.3735	0.0940

Q41: Does education affect ITA confidence?

Dependent variable: Confidence

Regression Statistics	
R-Squared (Coefficient of Determination)	0.1051
Adjusted R-Squared	0.0857
Multiple R (Multiple Correlation Coefficient)	0.3242
Standard Error of the Estimates (SEy)	1.1388
Number of Observations	48

Regression Results		
	Intercept	Education
Coefficients	6.2659	0.5923
Standard Error	0.4209	0.2548
t-Statistic	14.8868	2.3247
p-Value	0.0000	0.0246
Lower 5%	5.4187	0.0794
Upper 95%	7.1131	1.1051

Test Statistics^{a,b}

	Confidence
Chi-Square	5.456
df	3
Asymp. Sig.	.141

a. Kruskal Wallis Test

b. Grouping Variable:
Education

Q43—46: Does age, gender, education, experience, affect the perception of information overload?

Dependent variable: InfoOvld

Regression Statistics

R-Squared (Coefficient of Determination)	0.0944
Adjusted R-Squared	0.0101
Multiple R (Multiple Correlation Coefficient)	0.3072
Standard Error of the Estimates (SEy)	1.1683
Number of Observations	48

Regression Results

	Intercept	Age	Gender	Education	Experience
Coefficients	2.1076	0.0019	0.4193	-0.4044	0.0219
Standard Error	0.7279	0.0181	0.4255	0.3126	0.0309
t-Statistic	2.8954	0.1074	0.9855	-1.2934	0.7085
p-Value	0.0059	0.9150	0.3299	0.2028	0.4825
Lower 5%	0.6396	-0.0345	-0.4388	-1.0348	-0.0405
Upper 95%	3.5755	0.0384	1.2775	0.2261	0.0843

Q47—50: Does age, gender, education, experience, affect the perception of social impact?

Dependant variable: Social Impact

Regression Statistics

R-Squared (Coefficient of Determination)	0.1135
Adjusted R-Squared	0.0000
Multiple R (Multiple Correlation Coefficient)	0.3370
Standard Error of the Estimates (SEy)	1.0872
Number of Observations	24

Regression Results

	Intercept	Age	Gender	Education	Experience
Coefficients	2.1164	-0.0130	0.4615	-0.0826	-0.0685
Standard Error	0.9228	0.0239	0.7105	0.6068	0.0634
t-Statistic	2.2934	-0.5432	0.6495	-0.1361	-1.0799
p-Value	0.0334	0.5933	0.5238	0.8932	0.2937
Lower 5%	0.1849	-0.0629	-1.0257	-1.3526	-0.2012
Upper 95%	4.0478	0.0370	1.9486	1.1874	0.0642

RESTRICTED VERSION OF THIS DISSERTATION

A restricted copy of this dissertation that includes Experimental Scenarios and References is available on Calhoun at <https://library.nps.edu/nps-theses>.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, 32 C.F.R. § 147.7 (2016).
- Albrecht, W. Howe, K and Romney, M. (1984). *Deterring fraud: The internal auditor's perspective*. Altomonte Springs, FL: The Institute of Internal Auditors' Research Foundation.
- Anderson, T., McKenzie, S.A., Blais, C. L., and Brutzman, D. (2014). Geospatial mapping of Internet protocol addresses for real-time cyber domain visual analytics and knowledge management using the global information network architecture. *National Cybersecurity Institute Journal*, 1 (2), 33–50.
- Ard, J. B., Bishop, M., Gates, C., & Sun, M. X. (2013). Information behaving badly. In *Proceedings of the 2013 Workshop on New Security Paradigms Workshop*, 107–118.
- Armerding, T. (2015, May 08). Behavioral analytics vs. the rogue insider. Retrieved June 12, 2017, from <http://www.csoonline.com/article/2920232/data-protection/uba-vs-the-rogue-insider.html?page=2>
- Asch, S. E. (1951). Effects of group pressure upon the modification and distortion of judgments. In H. Guetzkow (Ed.), *Groups, leadership, and men* (pp. 222–236). Pittsburgh, PA: Carnegie Press.
- Ashby, W. R. (1962). Principles of the self-organizing system. In H. Von Foerster and G. W. Zopf, Jr. (Eds.), *Principles of self-organization: Transactions of the University of Illinois Symposium* (pp. 255–278). London: Pergamon Press.
- Axelrad, E. T., Sticha, P. J., Brdiczka, O., & Shen, J. (2013). A Bayesian network model for predicting insider threats. *IEEE 2013 Security and Privacy Workshops (SPW), 2013 IEEE* (pp. 82–89). doi:10.1109/SPW.2013.35
- Baracaldo, N., & Joshi, J. (2013). An adaptive risk management and access control framework to mitigate insider threats. *Computers & Security*, 39, 237–254.
- Bates, M. J. (1999). The invisible substrate of information science. *Journal of the Association for Information Science and Technology*, 50(12), 1043–1050.
- Baugess, K. G., Chamberlain, J. R., Chung, S. K., and Kelly, R. F. (2014). Reactive aggregate model protecting against real-time threats (Master's thesis, Monterey, California: Naval Postgraduate School, Monterey, CA).
- Bawden, D., & Robinson, L. (2008). The dark side of information: overload, anxiety and other paradoxes and pathologies. *Journal of Information Science*, 35(2), 180–191.

- Becker, G. S., & Murphy, K. M. (1994). The division of labor, coordination costs, and knowledge. In G. Becker (Ed.), *Human capital: A theoretical and empirical analysis with special reference to education*, 3rd ed., (pp. 299–322). Chicago, IL: University of Chicago Press.
- Bejtlich, R. (2013). *The practice of network security monitoring: Understanding incident detection and response*. San Francisco, CA: No Starch Press.
- Benner, P. E., Tanner, C. A., & Chesla, C. A. (2009). *Expertise in nursing practice: Caring, clinical judgment, and ethics*. New York: Springer Publishing Company.
- Berlin, A., Brettler, M. Z., & Fishbane, M. A. (2004). *The Jewish study bible: Jewish publication society Tanakh translation*. New York: Oxford University Press.
- Bishop, M. Conboy, H. Huong, P. Simidchieva, B., Avrunin, G., Clarke, L., Osterweil, L., & Peisert, S. (2014, May). Insider threat identification by process analysis. *IEEE CS Security and Privacy Workshops (SPW)*, 251–264. doi: 10.1109/SPW.2014.40
- Bonner, S. E., & Sprinkle, G. B. (2002). The effects of monetary incentives on effort and task performance: Theories, evidence, and a framework for research. *Accounting, Organizations and Society*, 27, 303–345.
- Bonner, S., Hastie, R., Sprinkle, G., & Young, M. (2000). A review of the effects of financial incentives on performance in laboratory tasks: implications for management accounting. *Journal of Management Accounting Research*, 12, 19–64.
- Borko, H. (1968). Information science: What is it? *American Documentation*, 19(1), 3–5.
- Borum, R. (2000). Assessing violence risk among youth. *Journal of Clinical Psychology*, 56, 1263–1288.
- Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach for evaluating risk of targeted violence. *Behavioral Sciences and the Law*, 17(3), 323–337.
- Brackney, R. C., & Anderson, R. H. (2004, March). Understanding the insider threat. *Proceedings of a March 2004 Workshop*. Santa Monica, CA: Rand Corporation.
- Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., Bart, E., & Ducheneaut, N. (2012, May). Proactive insider threat detection through graph learning and psychological context. *IEEE CS Security and Privacy Workshops (SPW)*, 142–149. doi: 10.1109/SPW.2012.29
- Brem, S. K., & Rips, L. J. (2000). Explanation and evidence in informal argument. *Cognitive Science*, 24(4), 573–604.

- Brodbeck, F. C., Kerschreiter, R., Mojzisch, A., & Schulz-Hardt, S. (2007). Group decision making under conditions of distributed knowledge: The information asymmetries model. *Academy of Management Review*, 32(2), 459–479.
- Brooks, F. (1995). *The mythical man-month* (Anniversary ed.). Boston, MA: Addison Wesley Publishing Company.
- Burns, C. S., & Bossaller, J. (2012). Communication overload: A phenomenological inquiry into academic reference librarianship. *Journal of Documentation*, 68(5), 597–617.
- Campbell, D., & Stanley, J. (1963). *Experimental and quasi-experimental designs for research*. Boston, MA: Houghton Mifflin.
- Campbell, W. B. (2017). Systems of Systems Approach to Insider Threat. (Master's thesis, Naval Postgraduate School, Monterey, CA).
- Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, sabotage, fraud)*. Boston, MA: Addison-Wesley.
- Carnap, R. (1956). The foundations of science and the concepts of psychology and psychoanalysis. In H. Feigl, M. Scriven (Eds.), *Minnesota studies in the philosophy of science*, Vol. 1 (pp. 38–43). Minneapolis, MN: University of Minnesota Press.
- Carney, R. M., & Marshall-Mies, J. (2000 September). *Adjudicative guidelines and investigative standards in the Department of Defense* (PERSEREC Technical Report-00-2). Monterey, CA: Defense Personnel Security Research Center.
- Catrantzos, N. (2012). *Managing the Insider Threat: No Dark Corners*. New York, NY: Taylor & Francis Group.
- Chaffetz, J., Meadows, M., Hurd, W. (2016, September). *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*. U.S. House of Representatives Committee on Oversight and Government Reform, 114th Congress. Retrieved from: <https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf>.
- Cheung, S. L., & Palan, S. (2012). Two heads are less bubbly than one: Team decision-making in an experimental asset market. *Experimental Economics*, 15(3), 373–397.
- Chewing, E., & Harrell, A. (1990). The effect of information load on decision makers' cue utilization levels and decision quality in a financial distress decision task. *Accounting, Organizations and Society*, 15(6), 517–542.

- Chidambaram, L., & Jones, B. (1993). Impact of communication medium and computer support on group perceptions and performance: A comparison of face-to-face and dispersed meetings. *MIS Quarterly*, 17(4), 465–491.
- Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. (2005, June). Towards a theory of insider threat assessment. In *Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05)* (pp. 108–117). doi:10.1109/DSN.2005.94
- Coburn, T. A. (2015, January). *A review of the Department of Homeland Security's missions and performance*. U.S. Senate Committee on Homeland Security and Governmental Affairs, 113th Congress. Retrieved from: <http://www.hsdl.org/?view&did=761088>
- Coffey, A. (2015, October). *Evaluating intelligence and information sharing networks : Examples from a study of the national network of fusion centers* (Issue Brief No. 2015–04). Washington, DC: The George Washington University Center for Cyber and Homeland Security.
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.
- Cole, E., & Ring, S. (2006). *Insider threat: Protecting the enterprise from sabotage, spying, and theft*. Sebastapol, CA: Syngress Publishing.
- Contos, B. T. (2006). *Enemy at the water cooler: True stories of insider threats and enterprise security management countermeasures*. Sebastapol, CA: Syngress Publishing.
- Cosgrove, K. P., Mazure, C. M., & Staley, J. K. (2007). Evolving knowledge of sex differences in brain structure, function, and chemistry. *Biological Psychiatry*, 62(8), 847–855.
- Cressey, D. R. (1953). *Other People's Money; A Study of the Social Psychology of Embezzlement*. New York, NY: Free Press.
- Creswell, J. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, CA: Sage Publications.
- Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*. London: Sage Publications.
- Cukrowski, J., & Baniak, A. (1999). Organizational restructuring in response to changes in information-processing technology. *Review of Economic Design*, 4(4), 295–305.

- Daft, R. L. (2001). *Essentials of organization theory and design*. Mason, OH: South Western Educational Publishing.
- Daft, R. L. (2007). *Principles of organization theory and design*. Belmont, CA: Thomson Publishing.
- Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Management science*, 32(5), 554–571.
- Davies, H.J., & Plotkin, M.R. (2005). *Protecting your community from terrorism: Strategies for local law enforcement (Vol. 5)*. Washington, DC: Police Executive Research Forum and U.S. Department of Justice Office of Community Oriented Policing. Retrieved from: http://media.cygnus.com/files/base/OFCR/document/2012/01/protectinglocalcommunitiesv5_10619254.pdf
- de Pillis, E., Furumo, K., Ray, J., Furumo, H., & Higa, K. (2015). Deadbeats in virtual teams: How gender, conscientiousness, and individualism/collectivism impact performance. *International Journal of Business and Information*, 10(3), 273–294.
- Dempsey, L. (2008). Always on: Libraries in a world of permanent connectivity. *First Monday*, 14(1).
- Denby, E., & Gammack, J. (1999). Modelling ignorance levels in knowledge-based decision support. In *Proceedings of 2nd Western Australian Workshop on Information Systems Research*.
- Dennis, A. R., Fuller, R. M., & Valacich, J. S. (2008). Media, tasks, and communication processes: A theory of media synchronicity. *MIS Quarterly*, 32(3), 575–600.
- Department of Defense Directive (DoDD) 5205.16. (2014, September 30). *The DOD insider threat program*. (DOD Directive 5205.16). Washington, DC: Work, R. Retrieved from <https://www.dtic.mil/whs/directives/corres/pdf/520516p.pdf>
- Dolk, D., Anderson, T., Busalacchi, F., and Tinsley, D. (2012, January). GINA: System interoperability for enabling smart mobile system services in network decision support systems. *2012 45th Hawaii International Conference on System Science (HICSS)*, 1472–1481). doi: 10.1109/HICSS.2012.293
- Domingos, P. (2015). *The master algorithm: How the quest for the ultimate learning machine will remake our world*. New York, NY: Basic Books.
- Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley Jr, R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 27(2), 555–579.
- Dreyfus, H., Dreyfus, S. (1986). *Mind over machine: The power of human intuition and expertise in the era of the computer*. New York, NY: Simon and Schuster.

- Dreyfus, S. E. (2004). The five-stage model of adult skill acquisition. *Bulletin of Science, Technology & Society*, 24(3), 177–181.
- Drucker, P. (1988). The coming of the new organization. *Harvard Business Review*, 66(1), 45–53.
- Edmunds, A., & Morris, A. (2000). The problem of information overload in business organisations: A review of the literature. *International Journal of Information Management*, 20(1), 17–28.
- Eppler, M. J., & Mengis, J. (2004). The concept of information overload: A review of literature from organization science, accounting, marketing, MIS, and related disciplines. *The Information Society*, 20(5), 325–344.
- Ertmer, P. A., & Newby, T. J. (2013). Behaviorism, Cognitivism, Constructivism: Comparing Critical Features From an Instructional Design Perspective. *Performance Improvement Quarterly*, 26(2), 43–71.
- Everett, S., Price, J., Bedwell, A., & Telljohann, S. (1997). Incentive in survey research.pdf. *Evaluation & The Health Professions*, 20(2), 207–214.
- Exec. Order No. 12968, 3 C.F.R. 40245 (1995)
- Exec. Order No. 13587, 3 C.F.R. 63811 (2011)
- Faber, S. (2015). *Use-case-based assessment of insider threat data sources* (Carnegie Mellon University/Software Engineering Institute-2015-SR-005). U Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute.
- Farace, R., Monge, P. R., & Russell, H. M. (1977). *Communicating and organizing*. New York, NY: Random House.
- Farnsworth, P. R., & Williams, M. F. (1936). The accuracy of the median and mean of a group of judgments. *The Journal of Social Psychology*, 7(2), 237239.
- Feigl, H. (1970). Beyond peaceful coexistence. In R.H. Stewart (Ed.), *Minnesota studies in the philosophy of science* (Vol. 5). Minneapolis, MN: University of Minnesota Press.
- Fein, R. A., & Vossekuil, B. (1998). Protective intelligence and threat investigations: A guide for state and local law enforcement officials (NCJ 170612). Washington, DC: U.S. Department of Justice.
- Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics*. Thousand Oaks, CA: SAGE Publications.

- FireEye. (2013). Big threats for small businesses: Five reasons your small or midsize business is a prime target for cybercriminals. Retrieved from <http://www2.fireeye.com/rs/fireeye/images/fireeye-smb-five-reasons.pdf>
- Fischer, E. A. (2016). *Cybersecurity Issues and Challenges: In Brief* (CRS Report No. R43831). Retrieved from Congressional Research Service website: <https://fas.org/sgp/crs/misc/R43831.pdf>
- Fiske, S. T., & Taylor, S. E. (1991). *Social cognition, 2nd*. New York, NY: McGraw-Hill.
- Freeman, S., Walker, M. R., Borden, R., & Latane, B. (1975). Diffusion of responsibility and restaurant tipping: Cheaper by the bunch. *Personality and Social Psychology Bulletin*, 1(4), 584–587.
- Galbraith, J. R. (1973). *Designing complex organizations*. Boston, MA: Addison Wesley Publishing Company.
- Galbraith, J. R. (1974). Organization design: An information processing view. *Interfaces*, 4(3), 28–36.
- Galbraith, J. R. (1977). *Organization design*. Boston, MA: Addison Wesley Publishing Company.
- Garst, R. D., & Gross, M. L. (1997). On becoming an intelligence analyst. *Defense Intelligence Journal*, 6(2), 47–59.
- Gavai, G. Sricharan, K. Gunning, D. Hanley, J. Singhal, M. and Rolleston, R. (2015). Supervised and Unsupervised methods to detect Insider Threat from Enterprise Social and Online Activity Data. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 6(4), 47–63.
- German, M., & Stanley, J. (2007, December). *What's wrong with fusion centers?* Washington, DC: American Civil Liberties Union. Retrieved from: https://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf
- Giere, R. (1991). *Understanding scientific reasoning* (3rd ed.). Fort Worth, TX: Holt, Rinehart, and Winston.
- Gigerenzer, G. (2001). *Bounded rationality: The adaptive toolbox*. Cambridge, MA: MIT Press. Retrieved from <http://www.princeton.edu/~smeunier/JonesBounded1.pdf>
- Gladwell, M. (2008). *Outliers: The story of success*. Boston, MA: Little, Brown and Company.
- Glaser, B., & Strauss, A. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Chicago, IL: Publishing Company.

- Godfrey-Smith, P. (2003). *Theory and reality: An introduction to the philosophy of science*. Chicago, IL: University of Chicago Press.
- Goldberg, H. G., Young, W. T., Memory, A., & Senator, T. E. (2016, January). Explaining and Aggregating Anomalies to Detect Insider Threats. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 2739–2748). IEEE.
- Goldenkoff, R. (2015). *Federal workforce: OPM and agencies need to strengthen efforts to identify and close mission—critical skills gaps* (GAO-15-223). Washington, DC: Government Accountability Office. Retrieved from <http://gao.gov/assets/670/668202.pdf>
- Goldratt, E. and Cox, J., (2016). *The Goal*. New York, NY: Routledge.
- Gordon, A. S. (2016, March). Commonsense Interpretation of Triangle Behavior. In *Thirtieth AAAI Conference on Artificial Intelligence*.
- Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, 17, 109–122.
- Graziano, A. M., & Raulin, M. L. (1993). *Research methods: A process of inquiry*. New York, NY: HarperCollins.
- Greitzer, F. L., & Ferryman, T. A. (2013, May). Methods and metrics for evaluating analytic insider threat tools. *IEEE CS Security and Privacy Workshops (SPW)*, 90–97. doi: 10.1109/SPW.2013.34
- Griffeth, R. W., Carson, K. D., & Marin, D. B. (1988). Information overload: A test of an inverted U hypothesis with hourly and salaried employees. In *Academy of Management Proceedings Vol. 1988, No. 1* (pp. 232–236). Briarcliff Manor, NY: Academy of Management.
- Griffiths, T. L., & Tenenbaum, J. B. (2009). Theory-based causal induction. *Psychological Review*, 116(4), 661–716.
- Guido, M. D., & Brooks, M. W. (2013). Insider threat program best practices. *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 1831–1839).
- Guilford, J. P., & Fruchter, B. (1973). *Fundamental statistics in psychology and education*. New York, NY: McGraw-Hill.
- Haase, R. F., Jome, L. M., Ferreira, J. A., Santos, E. J. R., Connacher, C. C., & Sendrowitz, K. (2014). Individual differences in capacity for tolerating information overload are related to differences in culture and temperament. *Journal of Cross-Cultural Psychology*, 45(5), 728–751.

- Hammer, M., & Champy, J. (1993). *Reengineering the corporation*. New York, NY: Harper Collins.
- Hanson, N. (1958). Observation. *Patterns of discovery*. New York, NY: Cambridge University Press.
- Harkins, S. G., Latane, B., & Williams, K. (1980). Social loafing: Allocating effort or taking it easy? *Journal of Experimental Social Psychology*, 16(5), 457–465.
- Harvey, J. H., & Weary, G. (1984). Current issues in attribution theory and research. *Annual review of psychology*, 35(1), 427–459.
- Harvey, P., Madison, K., Martinko, M., Crook, T. R., & Crook, T. A. (2014). Attribution theory in the organizational sciences: The road traveled and the path ahead. *The Academy of Management Perspectives*, 28(2), 128–146.
- Heath, C., & Heath, D. (2006). The curse of knowledge. *Harvard Business Review*, 84(12), 20–23.
- Heath, C., & Staudenmayer, N. (2000). Coordination neglect: How lay theories of organizing complicate coordination in organizations. *Research in Organizational Behavior*, 22, 153–191.
- Heider, F. (1958) *The psychology of interpersonal relations*. New York, NY: Wiley.
- Hempel, C. (1966). The role of induction in scientific inquiry. *Philosophy of Natural Science*. Upper Saddle River, NJ: Prentice-Hall.
- Hesse, M. (1970). Is there an independent observation language? In Robert G. Colodny (Ed.), *The nature and function of scientific theories* (pp. 36–70). Pittsburgh, PA: University of Pittsburgh Press.
- Heuer, R. J. (1999) *Psychology of Intelligence Analysis*. Center for the Study of Intelligence, Central Intelligence Agency.
- Hinds, P. J. (1999). The curse of expertise: The effects of expertise and debiasing methods on prediction of novice performance. *Journal of Experimental Psychology: Applied*, 5(2), 205.
- Holtzman, S. (1988). *Intelligent decision systems*. New York, NY: Addison-Wesley Longman Publishing Co., Inc..
- Housel, T., & Waldhard, E. (1981). The effects of communication load and mode on perceived decision quality and satisfaction. *Southern Speech Communication Journal*, 46(4), 361–376.

- Hughes, M.A., Price, R.L., & Marrs, D.W. 1986. Linking theory construction and theory testing: Models with multiple indicators of latent variables. *The Academy of Management Review*, 11(1).
- Hume, D. (2004). *An enquiry concerning human understanding*. Mineola, NY: Dover Publications.
- Hunker, J., & Probst, C. W. (2011). Insiders and insider threats—An overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2(1), 4–27.
- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1, 80.
- IBM Corporation. (2015). IBM 2015 Cyber security intelligence index: Analysis of cyber attack and incident data from IBM's worldwide security services operations. (Research report SEW03073-USEN-01). Retrieved from: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEW03073USEN>
- Ingham, A. G., Levinger, G., Graves, J., & Peckham, V. (1974). The Ringelmann effect: Studies of group size and group performance. *Journal of Experimental Social Psychology*, 10(4), 371–384.
- Internet Crime Complaint Center. (September, 2014). Increase in insider threat cases highlight significant risks to business networks and proprietary information. Retrieved from <https://www.ic3.gov/media/2014/140923.aspx>
- Irvine, D. N. (2016, September). *ExtendSim Simulation of the Navy insider threat hub* [Technical Report]. Naval Postgraduate School.
- Iselin, E. R. (1988). The effects of information load and information diversity on decision quality in a structured decision task. *Accounting, Organizations and Society*, 13(2), 147–164.
- Jackson, B. A. (2014). *How do we know what information sharing is really worth? Exploring methodologies to measure the value of information sharing and fusion efforts*. Kobo Books. Retrieved from: <https://www.kobo.com/us/en/ebook/how-do-we-know-what-information-sharing-is-really-worth-exploring-methodologies-to-measure-the-value-of-information-sharing-and-fusion-efforts>
- Jackson, T. W., & Farzaneh, P. (2012). Theory-based models of factors affecting information overload. *International Journal of Information Management*, 32(6), 523–532.
- Jaquith, A. (2007). *Security metrics*. Boston, MA: Addison Wesley.

- Jarvenpaa, S.L. 1988. The importance of laboratory experimentation in IS research (technical correspondence). *Communications of the ACM*, 31(12), 1502–1504.
- Johnson, T. (2006). *Forensic computer crime investigation*. Boca Raton, FL: CRC Press.
- Karau, S. J., & Williams, K. D. (1993). Social loafing: A meta-analytic review and theoretical integration. *Journal of Personality and Social Psychology*, 65(4), 681.
- Karr-Wisniewski, P., & Lu, Y. (2010). When more is too much: Operationalizing technology overload and exploring its impact on knowledge worker productivity. *Computers in Human Behavior*, 26(5), 1061–1072.
- Katz-Navon, T. Y. (2005). When collective- and self-efficacy affect team performance: The role of task interdependence. *Small Group Research*, 36(4), 437–465.
- Kelley, H. H. (1973). The processes of causal attribution. *American psychologist*, 28(2), 107.
- Kelley, H. H., & Michela, J. L. (1980). Attribution Theory and Research. *Annual Review of Psychology*, 31, 457–501.
- Kelly, R. F. (2014). Automated cyber threat analysis and specified process using vector relational data modeling (Master's thesis, Naval Postgraduate School, Monterey, CA).
- Kelly, R. F., & Anderson, T. S. (2016, May 12). A vector relational data modeling approach to Insider threat intelligence. *SPIE Proceedings 9831 Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VII*, 98310W. doi: 10.1117/12.22242299
- Kerlinger, F. N., & Lee, H. B. (2000). *Foundations of behavioral research*. Belmont, CA: Wadsworth.
- Kerr, N. L., & Tindale, R. S. (2004). Group performance and decision making. *Annual Review of Psychology*, 55(1), 623–655.
- Keysar, B. (1994). The illusory transparency of intention: Perspective taking in text. *Cognitive Psychology*, 26, 165–208.
- Klausegger, C., Sinkovics, R. R., & Zou, H. (2007). Information overload: A cross-national investigation of influence factors and effects. *Marketing Intelligence & Planning*, 25(7), 691–718.
- Klein, G. (1998). *Sources of power: How people make decisions*. Cambridge, Mass.: MIT Press.

- Klein, G., Moon, B., & Hoffman, R. F. (2006). Making sense of sensemaking: Alternative perspectives. *IEEE Intelligent Systems*, 21(4), 70–73.
- Kranacher, M. J., R. A. Riley Jr., and J. T. Wells. 2011. *Forensic Accounting and Fraud Examination*. New York, NY: John Wiley & Sons.
- Kravitz, D. A., & Martin, B. (1986). Ringelmann rediscovered: The original article. *Journal of Personality and Social Psychology*, 50(5), 936–941.
- Laczniak, R. N., DeCarlo, T. E., & Ramaswami, S. N. (2001). Consumers' responses to negative word-of-mouth communication: An attribution theory perspective. *Journal of consumer Psychology*, 11(1), 57–73.
- Larence, E. (2010). *Information Sharing: Federal agencies are helping fusion centers build and sustain capabilities and protect privacy, but could better measure results* (GAO-10-972). Washington, DC: Government Accountability Office. Retrieved from <http://www.gao.gov/assets/320/310268.pdf>
- Latané, B. (1981). The psychology of social impact. *American Psychologist*, 36(4), 343–356.
- Latané, B., & Dabbs Jr, J. M. (1975). Sex, group size and helping in three cities. *Sociometry*, 38(2), 180–194.
- Latané, B., & Darley, J. M. (1970). *The unresponsive bystander: Why doesn't he help?* Englewood Cliffs, NJ: Prentice Hall.
- Latané, B., Williams, K., & Harkins, S. (1979). Many hands make light the work: The causes and consequences of social loafing. *Journal of Personality and Social Psychology*, 37(6), 822–832.
- Law, A. M., & Kelton, W. D. (1991). *Simulation modeling and analysis* (2nd ed.). New York, NY: McGraw-Hill.
- Leavitt, H. J. (1965). Applied organizational change in industry: Structural, technological and humanistic approaches. In J. G. March (Ed.), *Handbook of organizations* (pp. 1144–1170). Chicago, IL: Rand McNally.
- Lenz, R.T. 1981. 'Determinants' of organizational performance: An interdisciplinary review. *Strategic Management Journal*, 2(2), 131–154.
- Levitt, R. E., Thomsen, J., Christiansen, T. R., Kunz, J. C., Jin, Y., & Nass, C. (1999). Simulating project work processes and organizations: Toward a micro-contingency theory of organizational design. *Management Science*, 45(11), 1479–1495.

- Libicki, M., & Pfleeger, S. (2004). Collecting the dots: Problem formulation and solution elements. Santa Monica: Rand Corporation.
- Liden, R. C., Wayne, S. J., Jaworski, R. A., & Bennett, N. (2004). Social loafing: A field investigation. *Journal of Management*, 30(2), 285–304.
- Lipton, P. (1993). Is the best good enough ? *Proceedings of the Aristotelian Society*, 93(May), 89–104.
- Lombrozo, T. (2007). Simplicity and probability in causal explanation. *Cognitive Psychology*, 55(3), 232–257.
- Long, J. S., & Ervin, L. H. (2000). Using Heteroscedasticity Consistent Standard Errors in the Linear Regression Model. *The American Statistician*, 54(3), 217–224.
- Maizlish, B., & Handler, R. (2005). IT (information technology) portfolio management step-by-step: Unlocking the business value of technology. New York, NY: John Wiley & Sons.
- Manis, M., Fichman, M., & Platt, M. B. (1978). Cognitive integration and referential communication: Effects of information quality and quantity in message decoding. *Organizational Behavior and Human Performance*, 22(3), 417–430.
- Mao, A., Mason, W., Suri, S., & Watts, D. J. (2016). An experimental study of team size and performance on a complex task. *PloS One*, 11(4), e0153048.
- March, J. G., & Simon, H. A. (1958). *Organizations*. New York, NY: Wiley-Blackwell.
- March, J., & Olsen, J. 1976. *Ambiguity and choice in organizations*. Bergen, Norway: Univer- sitetsforlaget.
- Marler, L. E., & Marrett, K. (2013). Feedback distractions during computer-mediated group collaboration. *Journal of Managerial Issues*, XXV(2), 172–191.
- Mascolo, R. (2016). Insider threat operations: Is collaboration a key factor? (Master's thesis) Naval Postgraduate School, Monterey, CA.
- Matloff, N. (2011). The art of R programming: A tour of statistical software design. San Francisco: No Starch Press.
- Maybury, M., Chase, P., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T., Wood, B., Sibley, C., Marin, J., Longstaff, T., Spitzner, L., Haile, J., Copeland, J., & Lewandowski, S. (2005, May). Analysis and detection of malicious insiders. Paper presented at the International Conference on Intelligence Analysis, McLean, VA.

- Mayo, E. (1933). The Hawthorne experiment. In E. E. Mayo (Ed.), *The human problems of industrial civilization* (pp. 53–94). Boston: Harvard University Press.
- McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data. The management revolution. *Harvard Business Review*, 90(10), 61–67.
- McAfee. (2014). Estimating the Global Cost of Cybercrime, Economic Impact of Cybercrime II. *Center for Strategic and International Studies*.
- McCarthy, J. (1980). Circumscription - A Form of Nonmonotonic Reasoning. *Artificial Intelligence*, 13, 27–39.
- McClure, S., Scambray, J., & Kurtz, G. (2012). Hacking exposed: Network security secrets and solutions (7th ed.). New York, NY: McGraw-Hill/Osborne.
- McNamara, M. R. (2000). Dysfunction in cyberspace: The insider threat. In A. D. Campen & D. H. Dearth (Ed.), *CyberWar 3.0: Human factors in information operations and future conflict* (pp. 75–85). Fairfax, VA: AFCEA International Press.
- Mead, D., & Moseley, L. (2001). Considerations in using the delphi approach: design, questions and answers. *Nurse Researcher*, 8(4), 24–37.
- Meadow, C. T., & Yuan, W. (1997). Measuring the impact of information: Defining the concepts. *Information Processing & Management*, 33(6), 697–714.
- Meadows, B., Langley, P., & Emery, M. (2014). An abductive approach to understanding social interactions. *Advances in Cognitive Systems*, 3, 87–106.
- Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63(2), 81.
- Mintzberg, H. (1980). Structure in 5's: A synthesis of the research on organization design. *Management Science*, 26(3), 322–341.
- Mitroff, I., & Linstone, H. (1993). The unbounded mind: Breaking the chains of traditional business thinking. Oxford: Oxford University Press.
- Moore AP, Cappelli DM, & Trzeciak RF. (2008). The 'big picture' of insider IT sabotage across U.S. critical infrastructures. (Carnegie Mellon University/Software Engineering Institute Technical Report-009). Retrieved from: <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8703>
- Morales, J., Gendron, Y., & Guénin-Paracini, H. (2014). The construction of the risky individual and vigilant organization: A genealogy of the fraud triangle. *Accounting, Organizations and Society*, 39(3), 170–194.

- Mulvey, P., & Klein, H. (1998). The impact of perceived loafing and collective efficacy on group goal processes and group performance. *Organizational Behavior and Human Decision Processes*, 74(1), 62–87.
- Mun, J. (2015). *Modeling Risk*, (3rd ed.). Dublin, CA: Thompson-Shore and ROV press.
- Musgrave, A. (1988). The ultimate argument for scientific realism. In R. Nola (Ed.), *Relativism and realism in science*. Dordrecht, The Netherlands: Kluwer Academic Publishers.
- Nadler, D. A., & Tushman, M. L. (Autumn 1980). A model for diagnosing organizational behavior: Applying a congruence model. In *Organizational Dynamics*, 9(2), 35–51.
- National Insider Threat Task Force. (2014, March 14). *Clarification of enterprise audit management (EAM), user activity monitoring (UAM), continuous monitoring, and continuous evaluations* (NITTF-2014-008). Retrieved from https://www.ncsc.gov/nitff/docs/EAM_UAM_and_Continuous_Monitoring_Definitions-Signed.pdf
- National Science and Technology Council. (2016). Federal cybersecurity research and development strategic plan. Retrieved from https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf
- NetDiligence. (2016). NetDiligence 2015 cyber claims study. Retrieved from https://netdiligence.com/wp-content/uploads/2016/05/NetDiligence_2015_Cyber_Claims_Study_093015.pdf
- Newman, I., & Benz, C. R. (1998). *Qualitative-quantitative research methodology: Exploring the interactive continuum*. Carbondale, IL: Southern Illinois University Press.
- Newton, L. (1990). Overconfidence in the communication of intent: Heard and unheard melodies. (Unpublished doctoral dissertation) Stanford University, Stanford, CA.
- Nielson, M. (2012). *Reinventing discovery: The new era of networked science*. Princeton, NJ: Princeton University Press.
- Nonaka, I., Toyama, R., & Nagata, A. 2000. A firm as a knowledge-creating entity: A new perspective on the theory of the firm. *Industrial and Corporate Change*, 9(1), 1–20.
- O'Reilly, C. A. (1980). Individuals and information overload in organizations: Is more necessarily better?. *Academy of Management Journal*, 23(4), 684–696.

- Oliveira, A. (2007). A Discussion of Rational and Psychological Decision-Making Theories and Models : The Search for a Cultural-Ethical Decision-Making Model. *Journal of Business Ethics*, 12(2), 1478–82.
- Oltramari, A., Ben-Asher, N., Cranor, L., Bauer, L., & Christin, N. (2014, October). General requirements of a hybrid-modeling framework for cyber security. In 2014 IEEE Military Communications Conference (pp. 129–135). IEEE.
- Oltsik, J. (2013). *The Vormetric/ESG insider threat report*. Retrieved from <http://go.thalesecurity.com/rs/vormetric/images/The-Vormetric-Insider-Threat-Report-Oct-2013.pdf>
- Oppenheim, C. (1997). Managers' use and handling of information. *International Journal of Information Management*, 17(4), 239–248.
- Orcher, L. (2005). *Conducting research: Social and behavioral science methods*. Glendale, CA : Pyrczak Publishing.
- Pfleeger, S. L., Predd, J. B., Hunker, J., & Bulford, C. (2010). Insiders behaving badly: Addressing bad actors and their actions. *IEEE Transactions on Information Forensics and Security*, 5(1), 169–179.
- Piaget, J. (1954). *The construction of Reality in the Child*. New York, NY: Basic Books
Original French Edition, 1937
- Ponemon Institute. 2016. Cost of Cyber Crime Study: United States. Available from: <http://www.ibm.com/security/data-breach>.
- Popper, K. (1963). *Conjectures and refutations: The growth of scientific knowledge*. London: Routledge.
- Porter, L. W., Lawler, E. E., & Hackman, J. R. (1975). *Behavior in organizations*. New York, NY: McGraw-Hill.
- Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers and Security*, 30(6–7), 486–497.
- Proudfoot, J. G., Boyle, R., & Schuetzler, R. M. (2016). Man vs. machine: Investigating the effects of adversarial system use on end-user behavior in automated deception detection interviews. *Decision Support Systems*, 85, 23–33.
- Reddy, M., Borum, R., Berglund, J., Vossekuil, B., Fein, R., & Modzeleski, W. (2001). Evaluating risk for targeted violence in schools: Comparing risk assessment, threat assessment, and other approaches. *Psychology in the Schools*, 38(2), 157–172.

- Reichardt, R. (2006). Digital musings. *Internet Reference Services Quarterly*, 53(9), 1689–1699.
- Ringelmann, M. (1913). Recherches sur les moteurs animés: Travail de l'homme. *Annales de l'Institut National Agronomique*, 12(1), 1–40.
- Ritchie, S. J., Bates, T. C., & Deary, I. J. (2015). Is education associated with improvements in general cognitive ability, or in specific skills? *Developmental Psychology*, 51(5), 573–582.
- Robbins, T. L. (1995). Social loafing on cognitive tasks: An examination of the “sucker effect.” *Journal of Business and Psychology*, 9(3), 337–342.
- Roumani, A. Fung, C. Rai, S. & Xie, H. (2016). Value analysis of cyber security based on attack types. *ITMSOC: Transactions on Innovation and Business Engineering*, 1, 34–39.
- Ruben, B. (1975). *General systems theory and human communication*. Rochelle Park, N.J.: Hayden Books.
- Rubio-Fernández, P., & Glucksberg, S. (2012). Reasoning about other people's beliefs: Bilinguals have an advantage. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 38(1), 211.
- Samuelson, P., & Nordhaus, W. (2001). *Microeconomics*. New York, NY: Mcgraw-hill Publishing.
- Sanders, C., Randall, L., & Smith, J. (2014). *Applied network security monitoring: Using open source tools*. Waltham, MA: Syngress Publishing.
- Sanzgiri, A. and Dasgupta, D. (2016). Classification of insider threat detection techniques. *ACM 2016 Proceedings of the 11th Annual Cyber and Information Security Research Conference* (p. 25). doi:10.1145/2897795.2897799
- Saracevic, T. (1992). Information science: Origin, evolution and relations. In Vakkari, P. & Cronin, B. (Eds.), *Conceptions of library and information science: Historical, empirical and theoretical perspectives* (pp. 5–7). Los Angeles, CA: Taylor Graham.
- Sarkar, M. B., Butler, B., & Steinfield, C. (1995). Intermediaries and cybermediaries: A continuing role for mediating players in the electronic marketplace. *Journal of Computer-Mediated Communication*, 1(3), 1–14.
- Savolainen, R. (2007). Filtering and withdrawing: Strategies for coping with information overload in everyday contexts. *Journal of Information Science*, 33(May), 611–621.

- Savolainen, R. (2015). Cognitive barriers to information seeking: A conceptual analysis. *Journal of Information Science*, 41(5), 613–623.
- Scheibe, M., Skutsch, M., & Schofer, J. (1975). Experiments in delphi methodology. In H. A. Linstone & M. Turoff (Eds.), *The delphi method: Techniques and applications* (pp. 262–287). Boston, MA: Addison-Wesley.
- Schick, A., Gordon, L., & Haka, S. (1990). Information overload: A temporal approach. *Accounting, Organizations and Society*, 15(3), 199–220.
- Schippers, M. C. (2014). Social loafing tendencies and team performance: The compensating effect of agreeableness and conscientiousness. *Academy of Management Learning and Education*, 13(1), 62–81.
- Schroder, H. M., Driver, M. J., & Streufert, S. (1967). *Human information processing: Individuals and groups functioning in complex social situations*. New York, NY: Holt, Rinehart, & Winston.
- Schuchter, A., & Levi, M. (2016). The fraud triangle revisited. *Security Journal*, 29(2), 107–121.
- Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6), 526–531.
- Schwartau, W. (1999). *Time based security: Practical and provable methods to protect enterprise and infrastructure*. Seminole, FL: Interpact Press.
- Sellen, J. (2016). Insider threat data sharing. (Master's thesis, Naval Postgraduate School, Monterey, CA).
- Seng, J. M. (2016, May). Behavior-based network management: a unique model-based approach to implementing cyber superiority. Proceedings SPIE 9826 Cyber Sensing 2016,98260H).doi: 10.1117/12.2227969
- Shenk, D. (1997). Data smog: Surviving the info glut. *Technology Review*, 100(4), 18–26.
- Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T., & Flynn, L. (2012). *Common sense guide to mitigating insider threats, 4th edition* (Carnegie Mellon University/Software Engineering Institute-2012-TR-012). U Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute.
- Simon, B. (1979). *Functional integration and quantum physics* (Vol. 86). San Diego, CA: Academic Press.
- Simon, H. A. (1962). New developments in the theory of the firm. *The American Economic Review*, 52(2), 1–15.

- Simon, H. A. (1973). Applying information technology to organization design. *Public Administration Review*, 33(3), 268–278.
- Simon, H. A. (1996). *The sciences of the artificial*. Boston, MA: MIT Press.
- Simon, H. A. (2000). Bounded rationality in social science: Today and tomorrow. *Mind & Society*, 1(1), 25–39.
- Sirkin, M., (1999). *Statistics for the social sciences*. London: Sage Publications.
- Skinner, B. F. (1976). *About behaviorism*. New York, NY: Vintage.
- Smith, K. (1953). Distribution-free statistical methods and the concept of power efficiency. In Festinger, L. & Katz D. (Eds.), *Research methods in the behavioral sciences* (pp. 536–777). New York: Dryden Press.
- Sorkin, R., Hays, C., & West, R. (2001). Signal-detection analysis of group decision making. *Psychological Review*, 108(1), 183–203.
- Soucek, R., & Moser, K. (2010). Coping with information overload in email communication: Evaluation of a training intervention. *Computers in Human Behavior*, 26(6), 1458–1466.
- SPAWAR. (2015). U.S. Navy Insider Threat Program Analysis Overview, Summary, and Recommendations. CERT Insider Threat Center.
- Speier, C., Valacich, J. S., & Vessey, I. (1999). The Influence of task interruption on individual decision making: An information overload perspective. *Decision Sciences*, 30(2), 337–360.
- Spink, A. (2000). Toward a theoretical framework for information science. *Informing Science*, 3(2), 73–76.
- Staats, B. R., Milkman, K. L., & Fox, C. R. (2012). The team scaling fallacy: Underestimating the declining efficiency of larger teams. *Organizational Behavior and Human Decision Processes*, 118(2), 132–142.
- Starbuck, W.H., & Milliken, F.J. (1988). Executives' perceptual filters: What they notice and how they make sense. In D. C. Hambrick (Ed.), *The executive effect: Concepts and methods for studying top managers* (pp. 35–65). Greenwich, CT: JAI.
- Steiner, I. D. (1966). Models for inferring relationships between group size and potential group productivity. *Behavioral Science*, 11(4), 273–283.
- Steiner, I. D. (1972). *Group processes and group productivity*. New York: Academic Press.

- Stolovitch, H., Clark, R., & Condly, S. (2002). *Incentives, Motivation and Workplace Performance : Research & Best Practices*.
- Swanson, C. R., Chamelin, N. C., Territo, L., & Taylor, R. (1992). *Criminal investigation*. New York, NY: McGraw-Hill.
- Sweller, J. (1988). Cognitive load during problem solving: Effects on learning, *Cognitive Science* 12, 285, 257–285.
- Symantec. (2016). Internet security threat report (Vol. 21). Retrieved from <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>
- Taylor, J.R., & Van Every, E. J. 2000. *The emergent organization: Communication as its site and surface*. Mahweh, NJ: Erlbaum.
- Taylor, R. S. (1966). Professional aspects of information science and technology. *Annual Review of Information Science and Technology*, 1(15–40).
- Thagard, P. (1993). *Computational philosophy of science*. Cambridge, MA: MIT Press.
- Thompson, J. D. (1967). *Organizations in action: Social science bases of administrative theory*. Piscataway, NJ: Transaction Publishers.
- Thomson, W. (1889). *Popular lectures and addresses*. London: MacMillan and Company.
- Thorndyke, P. W., & Hayes-Roth, B. (1979). The use of schemata in the acquisition and transfer of knowledge. *Cognitive Psychology*, 11(1), 82–106.
- Tushman, M. L., & Nadler, D. A. (1978). Information processing as an integrating concept in organizational design. *Academy of Management Review*, 3(3), 613–624.
- Tuttle, B., & Burton, F. G. (1999). The effects of a modest incentive on information overload in an investment analysis task. *Accounting, Organizations and Society*, 24(8), 673–687.
- U.S. vs. Shahzad, 10 CR. 541 (MGC). (2010).
- U.S. vulnerabilities to money laundering, drugs and terrorist financing: HSBC case history*. Hearing before the Permanent Subcommittee on Investigations of the Committee on Homeland Security and Governmental Affairs. United States Senate, 112th Cong. 2(2012) (testimony of Carl Levin).

- Utin, D. M., Utin, M. A., & Utin, J. (2008). General misconceptions about information security lead to an insecure world. *Information Security Journal: A Global Perspective*, 17(4), 164–169.
- Verizon Inc. (2016). 2016 Data breach investigations report. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
- von der Gracht, H. A. (2008). The Delphi technique for futures research. *The Future of Logistics: Scenarios for 202* (pp. 21–68). Wiesbaden, Germany: GablerVerlag.
- Wang, T. (2013, May 13). Why big data needs thick data. [Web Log Post]. Retrieved from <http://ethnographymatters.net/blog/2013/05/13/big-data-needs-thick-data/>
- Weick, K. (1995). *Sensemaking in organizations*. Thousand Oaks, CA: Sage Publications.
- Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. *Organization science*, 16(4), 409–421.
- Weiner, B. (1972). Attribution theory, achievement motivation, and the educational process. *Review of educational research*, 42(2), 203–215.
- White House (2012). *National strategy for information sharing and safeguarding*. Retrieved from: https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf
- White House. (2007). National strategy for information sharing: *Successes and challenges in improving terrorism-related sharing*. Retrieved from: https://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf
- Wilshusen, G. C. (2014). *Information Security: Federal agencies need to enhance responses to data breaches*. (GAO-14-487T). Washington, DC: Government Accountability Office. Retrieved from <http://www.gao.gov/assets/670/662227.pdf>
- Wittkop, J. (2017, April 07). From the Office of the CTO: Building Effective Insider Threat Programs. Retrieved June 13, 2017, from <https://www.intelisecure.com/office-cto-building-effective-insider-threat-programs/>.
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38.
- Wu, M. M. (2005). Why print and electronic resources are essential to the academic law library. *American Association of Law Libraries Law Library Journal*, 97(233), 1–19.

- Yerkes, R. M., & Dodson, J. D. (1908). The relation of strength of stimulus to rapidity of habit formation. *Journal of Comparative Neurology and Psychology*, 18(5), 459–482.
- Yin, R. (2014). *Case study research*. Thousand Oaks, CA: Sage Publications.
- Young, W. Memory, A. Goldberg, H. & Senator, T. (2014). Detecting unknown insider threat scenarios. *IEEE 2014 Security and Privacy Workshops (SPW), 2014 IEEE* (pp. 277–288). doi:10.1109/SPW.2014.42
- Zins, C. (2006). Conceptions of Information Science. *Journal of the American Society for Information Science*, 58(3), 335–350.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California